Bachelor's thesis

International Business

2015

Heta Kuustie

MONEY LAUNDERING PREVENTION

– From International Standards to Finnish Banks

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR´S THESIS | ABSTRACT
TURKU UNIVERSITY OF APPLIED SCIENCES

International Business

2015| 71+6

Nicolas Le Grand

Heta Kuustie

MONEY LAUNDERING PREVENTION

– FROM INTERNATIONAL STANDARDS TO FINNISH BANKS

Money laundering is an international issue as the estimated amount of money laundered globally per year is 2-5% of the global GDP. Money laundering is a consequence of almost all profit generating crime, and thus can occur anywhere in the world. Many international instruments have been established to combat money laundering.

This thesis describes money laundering, money laundering prevention, and how Finnish banks are obliged by the law to prevent money laundering. The purpose of this thesis is not to look for a solution to a problem, but rather to come up with an information package on money laundering and the prevention of it. The reader is provided with detailed information on what measures banks must take in order to combat money laundering.

The Finnish anti-money laundering act is based on the EU rules. The EU rules are again based on international standards set by the Financial Action Task Force. The key principles of the Finnish anti-money laundering act are Customer Due Diligence and a risk-based approach. Banks must have sufficient information on their customers' activities, financial status, banking practices, and purpose for which the services are used. If banks recognize suspicious transactions, they must report them to the Financial Intelligence Unit, who further investigates the suspicion of money laundering.

This thesis is mainly a literature / law review where the most substantial information is gathered from various sources. A service manager of a Finnish bank is also interviewed to see how the law is applied in practice. Although the thesis is not written as an assignment given by a bank, it can be used as an orientation guide to money laundering prevention for new employees in the banking sector.

KEYWORDS:

Money laundering, anti-money laundering (AML), counter-terrorist financing (CTF), customer due diligence (CDD), suspicious transaction, bank

CONTENT

APPENDICES

FIGURES

TABLES

LIST OF ABBREVIATIONS

AML	Anti-money laundering
ATM	Automated Teller Machine
CDD	Customer Due Diligence
CTF	Counter-terrorist financing
EU	European Union
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FDI	Foreign Direct Investment
FIN-FSA	Finnish Financial Supervisory Authority
FIU	Financial Intelligence Unit
FSA	Financial Supervisory Authority
OECD	Organisation for Economic Cooperation and Development
PEP	Politically Exposed Person
PSP	Payment Service Provider
UN	United Nations

1 INTRODUCTION

I worked as a cashier service officer in a bank in the summer of 2015. Before that summer, I had never really thought about what money laundering actually is. Neither had I thought about all the anti-money laundering rules that apply to banks and various other service providers. When I started working at the bank, I was told about the anti-money laundering (AML) act, and how the bank is obliged by the law to know their customers and report suspicious transactions. As Customer Due Diligence (CDD) became a part of my everyday work, I thought it would be interesting to do more research about money laundering prevention, and to possibly write my thesis about the subject.

To put it in a nutshell, money laundering is the process of making illegally-gained funds appear legal. Due to the illegal nature of money laundering, it is difficult to estimate the total amount of money that goes through the laundry cycle (Sahavirta 2008, 38). There are no precise statistics available at all. However, according to the United Nations Office on Drugs and Crime, the estimated amount of money laundered globally per year is 2 – 5% of global GDP, or 800 billion – 2 trillion in US dollars (UNODC n.d.). Thus money laundering is a huge global issue. Money laundering is a consequence of almost all profit generating crime and can thus occur basically anywhere in the world (FATF n.d.). Globalization and rapidly developing technology has not only made money laundering easier for the criminals, but has also brought challenges to preventing money laundering.

If money laundering is left unchecked or dealt ineffectively, the possible social and political costs are serious. Criminals can acquire control of large sectors of the economy through investments, offer bribes to public officials, and infiltrate financial institutions. The economic and political influence of organized crime groups may weaken the social structure, collective ethical standards and democratic institutions. Most importantly, laundering enables criminal activity to continue. Many times, a money laundering investigation is the only way to locate the hidden assets and establish the identity of the criminals responsible.

(FATF n.d..) Therefore it is important to continue developing international AML standards and national legislation.

Criminals use, among others, financial service providers as intermediaries to launder their illicit funds. Banks are, among others, “parties subject to the reporting obligation”, which means that they are obliged to report suspicions of money laundering or terrorist financing to the Financial Intelligence Unit. Banks must know their customers well enough to be able to recognize unusual or suspicious transactions. Thus the key principles of the AML Act are CDD and a risk-based approach to money laundering and terrorist financing.

Although financing of terrorism has its own special aspects, is often considered to be just a part of money laundering. The techniques used for financing terrorism and laundering money are very similar. Terrorist financing and money laundering are often placed under the same title. Therefore the Finnish AML law is called “Act on Detecting and Preventing Money Laundering and Terrorist financing” (503/2008). However, I wanted to keep the thesis focused on money laundering and thus will only briefly define terrorist financing. Furthermore, money laundering and the prevention of it is a broad subject. Thus I wanted to highlight the main points of money laundering, and then focus on the AML legislation and how the law is applied in practice in banks. In order to keep the research focused, I also had to limit the handling of certain topics. In the last chapter, I will provide the reader with detailed information on how banks are obliged to combat money laundering.

1.1 Research objectives

The purpose of this thesis is not to look for a solution to a problem, but rather to present an overview on money laundering and what measures banks must take in order to prevent money laundering. The idea is to collect information from various sources in order to identify the main points in the anti-money laundering area. Although the thesis is not written as an assignment given by a contractor, it can be used as an orientation guide for new employees in the banking sector.

By the end of the thesis, the following research questions will be answered:

1. What are anti-money laundering laws?
2. How are banks obliged by the law to prevent money laundering?
3. How the AML Act is applied in practice in banks?
4. What does Customer Due Diligence involve?

Although money laundering prevention is important, the measures have also been criticized by different parties. In the end of the report, I will discuss the effectiveness of anti-money laundering laws and measures.

1.2 Structure of the thesis and research methods

The thesis is divided into three main sections: money laundering, money laundering prevention, and the role of a bank in applying AML/CTF measures. In order to understand the AML/CTF measures, the process of money laundering must be understood. The first part of the thesis is dedicated to defining money laundering, the laundering process, and the prevalence of money laundering. The second part is about money laundering prevention beginning with international standards which work as a basis for the EU legislation. The EU legislation, then again, works as a basis for the Finnish AML legislation. Finally, the last part goes into detail about the Finnish AML Act, and how the law is applied in practice in banks.

Different research methods are used in this thesis. However, this thesis is mainly about regulatory framework as it involves a lot of legal issues. Mainly secondary sources of information are used. The first part is largely a literature review where the most substantial information concerning money laundering is gathered. It slightly involves using quantitative methods, too, as statistics provided by the Finnish Financial Intelligence Unit are interpreted. The second part introduces the AML standards and laws starting from international level and then narrowing down to national legislation. Also the parties who the law applies to are introduced. In the second part, different organizations' webpages, and the EU Directive and Regulation itself, are used as sources of information. The Finnish AML Act is introduced in this section, too. In the third part, the AML Act

is looked more deeply into as it is used as a basis for answering the question “how banks are obliged by the law to prevent money laundering”. The standard 2.4 by Financial Supervisory Authority is used for giving concrete examples how the law should be applied.

I deployed qualitative research methods when conducting an in-depth interview in the third part of the thesis. I interviewed the service manager of a Finnish bank to get an insight how the bank applies the law. The interview was the most important primary source of information to this thesis. The interview questions were semi-structured, open-ended questions which enabled the interview to be more like a discussion. Due to the nature of preventing and detecting money laundering, the service manager could not give very exact answers to be published, though. However, I gathered the main points of the interview to support the theory.

Figure 1. Money-Laundering (Caon 2015).

2 MONEY LAUNDERING

What is nowadays referred to as “money laundering” is traditionally said to originate from Mafia ownership of laundromats in the U.S. According to the

traditional theory, gangs that generated illicit cash from criminal activities, such as prostitution, extortion and gambling, purchased legitimate businesses through which they funneled the dirty money. Whether the theory is true or not, the term stuck and is now commonly accepted when talking about the process of making illegally-gained proceeds appear legal. (Turner 2011, 2.)

It all stems from Al Capone, one of the biggest criminal leaders in the 1930s. Despite bootlegging whiskey and other crimes he committed, he was convicted of simple tax evasion. As gangsters saw what happened to Capone, they became more cautious with the origin, accounting and disbursement of their funds. Although the world is no longer the cash-based economy it used to be, the lessons that were learned by gangsters in attempting to avoid criminal prosecution are still used today. It has been said that Meyer Lansky, a major organized crime figure, developed the modern money laundering approach. The cash that was illegally gained in the U.S. was taken to Switzerland and then loaned back to the entities controlled and owned by gangsters themselves. The concept of “loan-to-back” is still a widely used mechanism for laundering cash; as with this route, the real timing of the illegally-gained funds is obscured. Also, it allows the launderers to declare and utilize cash while providing only limited resources for investigators. (Turner 2011, 2-3; Matonis 2013.)

2.1 Definition

Money laundering has been defined in various ways, depending on the source. The definitions used by regulators, law enforcements and criminal codes are mostly focused on either the accounting aspects or the criminal aspects (Turner 2011, 3). According to Doug Hopton, the author of Money Laundering: A Concise Guide For All Business (2009), people believe that money laundering can be described in one of the following ways: turning dirty money into clean money, washing drug money, or disguising criminal money. He states that although the historical description is fine as far as it goes, the term “money laundering” is a misnomer as it does not recognize that in the modern world, money laundering does not have to involve actual money. In the modern world,

“money laundering occurs every time any transaction takes place or relationship is formed which involves any form of property or benefit, whether it is tangible or intangible, which is derived from criminal activity” (Hopton 2009, 2). The fact that criminal proceeds do not actually have to be moved in order to be laundered should not be overlooked. For example, when legitimately earned money is placed into a bank in another country and the account holder fails to declare the income on a tax return in the country in which it was earned, the funds become returns of a crime. Thus the bank is laundering the funds without necessarily knowing it. Also, even in a relationship where there is no obvious process of receiving or paying money, laundering can still occur: there are cases where criminals’ primary objective is to disguise the fact that they own a property. By doing so, the criminals want to break the connection between themselves and the property that could possibly link them to the criminal offence. (Hopton 2009, 2.)

Jonathan Turner (2011), again states that most definitions of money laundering used by e.g. law enforcement agencies and regulators are incomplete to a proper understanding of the process. Traditionally, the money laundering process comprises three stages: placement, layering, and integration (Hopton 2009, 2-3; Turner 2011, 3). The issue is that these definitions also cover a lot of legitimate activities. According to Turner, creating an adequate definition is challenging due to the fact that the basic roles and actions are often disputed. He states that in a criminal trial, for example, the standard definitions are disputed as the prosecution tries to place the activities under the money laundering title; whereas the defense argues those to be merely common business activities. (Turner 2011, 3.) Although the world has changed and there has been economic globalization, it can be said that the basic idea in money laundering is still the same: making dirty money appear clean.

2.2 Terrorist financing

Financing of terrorism is considered by many to be just a part of money laundering. To some extent it is correct, however, it does have its own special

aspects. Terrorist organizations require money for e.g. training, materials and travel expenses, so it is vital to them to have international flows of funds which they can use for their aims. Although many different methods are used by terrorists to raise the funds they need, the methods generally fall into one of the two categories: 1. funds from the supporter states or organizations 2. fund-raising either from legitimate or illegitimate sources. Some examples of the second category are drug trafficking, people-smuggling, donations, charities and fundraising, kidnapping, and extortion. (Hopton 2009, 4-5.) As said, in the case of terrorist financing, funds can stem from both legal and illicit sources, whereas in the case of money laundering, the funds are always of illicit origin. The primary goal of individuals or organizations involved in the financing of terrorism is not necessarily to conceal the sources of money but to conceal both the financing and the nature of the financed activity. (IMF n.d..)

In both terrorist financing and money laundering, the actor makes an illegitimate use of the financial sector. The techniques used for financing terrorism and laundering money are very similar and in many cases identical. Therefore, an effective counter-terrorist financing (CTF) and anti-money laundering (AML) framework has to address both risk issues: it must detect, prevent and punish illegal funds entering the financial system; and the funding of terrorist individuals and organizations. CFT and AML strategies converge as they aim at attacking criminals and terrorists through their financial activities, and they both use the financial trail to identify the components of the terrorist or criminal network. Mechanisms need to be put in place to read all financial transactions, and to detect suspicious financial transfers. (IMF n.d..) Due to the similarity in measures taken to make illegitimate use of the financial sector, both terrorist financing and money laundering are often placed under the same title.

2.3 Where does laundered money come from?

The underlying crime that gives rise to the illegally-gained funds to be laundered is called a “predicate offence”. The initial focus on money laundering occurred at the same time with the drug trade; nowadays, the trafficking of illegal drugs is

still one of the most common predicate offences committed. However, the number of predicate offences, and thus the scope of AML law, has inflated since the 1990s. These predicate offences nowadays include, among others: narcotics, tax evasion, robbery, fraud, extortion, bribery, smuggling, counterfeiting, insider trading, price-fixing, the illegal trade in arms and people, and kidnapping. (Turner 2011, 7; Sharman 2011, 17.) However, in Finland, the predicate offence may be any committed crime, as long as it has brought economic benefit for the perpetrator (Poliisi n.d.). It is important to remember that money laundering is not limited to organized crime groups, but money laundering also appeals to lawyers, accountants, and other service providers who facilitate money laundering (Turner 2011, 27). For example, Russian underworld groups paid corrupted senior Bank of New York officials $1.8 million to launder $7 billion during a three-year period (Sharman 2011, 17). However, according to Mariano-Florentino Cuellar's research paper (2003) (as cited in Sharman 2007, 18), "rather than one set of criminals paying for the services of independent money launderers, it seems that most laundering is done in-house by the criminals who perpetrated the original predicate crime".

2.4 Three Stages

There is not only one way of laundering money or other property. Money laundering can range from the simple method of using money in the form in which it was acquired to extremely complex schemes involving a web of international businesses and investments. However, money laundering has traditionally been divided into three stages: placement, layering, and integration. These stages often occur simultaneously or overlap, although they can also be separate and distinct. (Hopton 2009, 2-3; Turner 2011, 8.) It all depends on the facilities of the launderer, the requirements of the criminals and the prevailing regulations linked to the effectiveness of the monitoring systems of the financial or regulated sector. Although the three-stage model is a convenient way of describing money laundering, it has been criticized to be too simplistic as it does not adequately cover all situations in which money laundering occurs.

(Hopton 2009, 3.) However, the traditional three stages are introduced in the following sections.

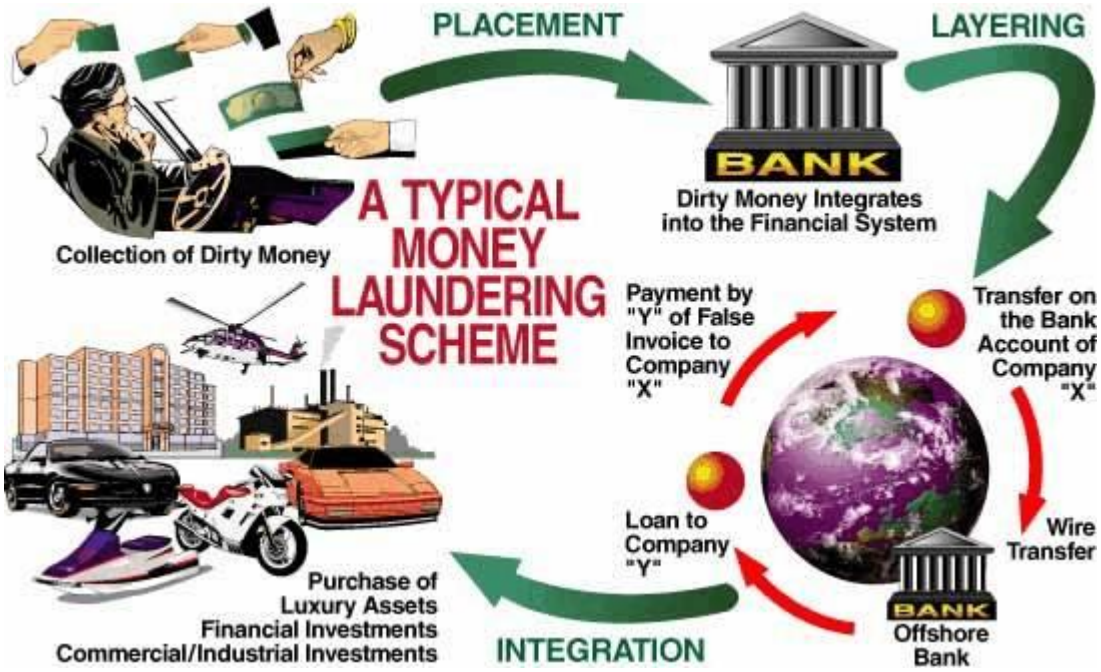

Figure 2. The Money-Laundering Cycle (UNODC n.d.).

2.4.1 Placement

The placement stage represents the initial entry of the illicit cash or proceeds of crime into the financial system. This stage serves two purposes: it relieves the criminal of holding and guarding large amounts of cash; and it places the money into the legitimate financial system. During the placement stage, money launderers are the most vulnerable to getting caught. This is because placing large amounts of money into the legitimate financial system may arise suspicions. (About Business Crime Solutions Inc. n.d..) Many laws and regulations concentrate on the prevention of money laundering, and therefore it is highlighted that financial service providers – as well as others subject to the reporting obligation – should recognize customers' unusual activities and report suspicious transactions. Thus it is important for service providers to know their customers and understand their conventional financial transactions. The AML legislation will be introduced later on.

The placement of the proceeds of crime can be done in many ways. The most common method is to deposit money into a financial account in a bank, an investment firm, or an insurance company. The money may also be shipped to a foreign financial organization to further obscure the path. (Turner 2011, 9.) Due to the AML laws, a large sum of money cannot be deposited into an account without raising suspicion. Thus launderer can use “smurfs” to defeat reporting threshold laws and avoid suspicion. This technique involves the use of many individuals, the smurfs, who in small and less conspicuous amounts exchange the illegally-gained proceeds for highly liquid items such as bank drafts and travelers cheques. These instruments are then given back to the launderer. Other methods for placement of funds are, for example, repayment of loans with illegal proceeds, purchase of gambling chips or placing bets on sporting events, purchase of foreign currency with illegal funds, and blending funds. Fund blending is a method where a legitimate cash focused business is used for co-mingling illicit funds with legitimate sales receipts. Another method for placement of funds is to use cash to buy works of art or other high-value items such as precious metals and jewelry. These items can be moved to a foreign country to be exchanged for cash, and the cash can then be deposited into a bank account in that country. (Sahavirta 2008, 24-31; About Business Crime Solutions Inc. n.d..)

The more organized the crime is, the more complex the money laundering process usually is. The proceeds of crime may get into the legal financial system through actions of so called gatekeepers. For example law firms may work as “professional enablers” providing legitimacy to the funds. They may place the illicit funds on the client accounts and then make transactions to third parties. (Sahavirta 2008, 30; Solicitors Regulation Authority 2014.) “Money laundered through law firms does not always involve actual legal transactions, and may instead involve passing the money through the client account to make it look legitimate, when no legal work has been undertaken” (Solicitors Regulation Authority 2014). Other legal parties, such as auditors and professional participants in the securities markets, may also become involved in

the criminal activities. (Sahavirta 2008, 30). Thus the AML legislation applies to attorneys, auditors and investment firms, too.

2.4.2 Layering

The second step in money laundering process, layering, involves stratifying the financial transaction. As the objective is to hide the illicit origins, the more layers are added to the process, the more difficult it will be to prove the illicit basis for the funds. At its simplest, layering is shifting the funds from one account to another, or moving them from one institution to another. Once the funds are in the financial system, it is rather easy to move them around the world. However, moving money from one account to another is easy to trace. To make tracing more difficult, criminals shift the money through various asset types although it incurs costs for buying and selling. Layers often include various financial accounts, high-value items, equipment and currency sales, and purchases of legitimate businesses. (Turner 2011, 9.)

Criminals may use loans or mortgages to layer and integrate illegally-gained funds into real estate and other high-value assets. For example, back-to-back loans are used. (Sahavirta 2008, 31.) “A back-to-back loan is a credit instrument under which funds or financial instruments are made available to the borrower. The bank receives collateral, whether direct or indirect, from the borrower’s own liquid assets. This occurs, for example, where a person has liquid assets and, instead of using them to meet his cash needs, raises a bank loan that is secured by the liquid assets in question” (De Nederlandsche Bank 2007). In the case of money laundering, the collateral is the illicit money placed in a third country. When the debtor fails to pay the debt, the bank realizes the collateral. (Sahavirta 2008, 31.) This way the criminal has documents to prove the source of the funds, which is the bank loan, and the bank that gave the loan gets its money back – or at least part of it – by realizing the collateral.

Some countries are structured to assist in these money laundering transactions. In these countries, legal and accounting firms often assist in setting up shell companies to help layering the transactions. Trusts and shell companies

disguise the true owner of the funds. In these countries, due to various bank secrecy laws, attorney-client privilege, and working with a local attorney, money launderers can move huge sums of money around the world. (Sahavirta 2008, 32-33; Turner 2011, 9.) Some of the most popular locations to hide cash include Cayman Islands, Bahamas, Monaco, Switzerland, Luxembourg, and Malta. When selecting an offshore location, money launderers consider many factors such as the strength of the secrecy laws, business language spoken, political climate, and the likelihood of extradition being facilitated by the local authorities. Many countries happily turn a blind eye to criminal acts as long as they have occurred elsewhere. To encourage cash-strong people to invest in their country, many governments have even passed various tax laws to encourage the migration of funds. Tax exemptions of foreign or investment income and payment of so called “past taxes” in return for citizenship or resident alien are examples of these kinds of inducements. Money launderers park their funds in international accounts to protect them from taxation, seizure, and the courts. (Turner 2011, 71-73.) Criminals may later ship the illicit funds back from these tax havens as foreign direct investments. This method is called “round-tripping”. (HG.org n.d..)

Due to the bank secrecy laws that often prevail in these tax havens, it is difficult to track the illicit funds. Once the criminal funds are placed in these tax havens, they are free to be used or transferred elsewhere. That’s why detecting also exports of funds from the home country is important.

Another method for layering the illegally-gained funds is over-invoicing (Sahavirta 2008, 32; Francis 2014). In her article “A Beginner’s Guide To Money Laundering” (2014), Diane Francis writes that “The real big shots don’t bother with casinos, crooked bank managers, junkets, or smurfs. They manage to transfer millions, or billions, without handling cash or involving banks at all, instead funneling their money through corporate deals (bribes, kickbacks, and embezzlement schemes), which are exempt from currency controls”. Ritva Sahavirta, the author of “Rahanpesu rangaistavana tekona” (2008), states that when over-invoicing, the two companies involved must have a common interest.

They may be commonly owned, for example. The two companies may be located in the same country, but usually the other one is registered offshore. They often do import/export business. The offshore company over-invoices company X for the exported goods, and the illegally-gained funds of company X are transferred to the offshore company. The difference between the actual value of the goods and the high price that was paid can be later on loaned back to company X. This way the illicit funds become laundered, and company X can prove that its incoming funds are originating from the loan given by the offshore company. (Sahavirta 2008, 32.) The more professional the money laundering is, the more complex the layering methods are. When using complex back-to-back loans and over-invoicing methods, it is probably about huge sums of “dirty” money.

2.4.3 Integration

The final stage of money laundering process integrates the seemingly legitimate funds into the perpetrators life. The income is returned to the criminal in a form that withstands ordinary scrutiny. (Sahavirta 2008, 33; Turner 2011, 9-10.) Having been placed initially as cash and layered through various financial transactions, the criminal funds are now fully integrated into the financial system and may be used for any purposes. The major objective at this stage is to reunite the money with the criminal without drawing attention. The money can be used for purchasing e.g. high-end automobiles, jewellery, property, and art work. (About Business Crime Solutions Inc. n.d..)

The methods used at this integration stage are defined slightly differently depending on the source. According to Turner (2011, 9), the integration stage has certain parity with the layering process. He states that one example of the integration methods is to use “front companies to ‘borrow’ funds from the foreign financial institution holding the illicit funds because the ‘loans’ are guaranteed by the deposits and the ‘lending’ institution faces no risk. Another common approach is the over-invoicing of goods or services, --.” Thus Turner places back-to-back loans and over-invoicing under the integration title. Sahavirta,

instead, places these activities under the layering title. However, as said earlier, the stages are not always separate and distinct, but can occur simultaneously or overlap. Therefore it is not always clear what activity goes under each title. Maybe, in today's world, it is not even necessary to try to categorize money laundering activities under different titles.

2.5 Modern money laundering methods

Money laundering is increasingly becoming a cybercrime as modern criminals are focusing on the internet. Technology in a rapidly changing financial environment facilitates the movement of criminals' money. (Turner 2011, 89; MIT Technology Review 2013.) Modern methods of money laundering make tracing the illicit funds increasingly difficult.

In a short period of time, virtual currencies, such as Bitcoin, have developed into a powerful payment method. Whereas virtual currencies offer an innovative, flexible and cheap method of payment, its unique business model poses a challenge to regulators around the world. The policy responses vary significantly: some countries embrace this new technology while others severely or totally limit its legitimate use. The Financial Action Task Force (FATF) conducted a research into the characteristics of virtual currencies to make an initial assessment of the money laundering and terrorist financing risk associated with this payment method. When it comes to legitimate use of virtual currencies, they offer many benefits such as lower transaction costs and increased payment efficiency. They also facilitate international payments. However, the FATF found that virtual currencies have certain characteristics, coupled with their global reach, that present potential money laundering and terrorist financing risks.

These risks include:

- Anonymity provided by the trade in virtual currencies on the internet

- Limited identification and verification of participants
- Lack of clarity regarding the responsibility for AML/CFT compliance, supervision and enforcement for these transactions that are segmented across several countries
- Lack of a central oversight body

According to the FATF's report on virtual currencies, this virtual payment method has already been abused for money laundering purposes. (FATF 2014.)

Another increasingly common method to launder money in today's world is to use online gaming. In a number of online games, it is possible to convert money from the real world into virtual goods or services. These virtual goods or services can then be converted back into real money. Popular games for scam like this include Second Life and World of Warcraft. (MIT Technology Review 2013.)

In addition to so called mule scams, where individuals' accounts are used for transferring large amounts of money, there are scams where people are offered jobs in which they can make significant income working from home. The "job" involves accepting money transfers into their accounts and then transferring these funds on to accounts set by the "employer". (MIT Technology Review 2013.) Modern money laundering methods also include using phones and smartcards, but I won't go into further detail about them in this thesis. However, as technology becomes more developed all the time, criminals constantly come up with new methods for laundering money.

2.6 Money laundering globally

Due to the illegal nature of money laundering, it is difficult to estimate the total amount of money that goes through the laundry cycle (Sahavirta 2008, 38). There are no precise statistics available at all. According to the United Nations Office on Drugs and Crime, the estimated amount of money laundered globally per year is 2 – 5% of global GDP, or 800 billion – 2 trillion in US dollars.

(UNODC n.d..) However, these estimates should be treated with caution as they are only intended to give an estimate of the extent of money laundering (FATF n.d.).

Money laundering is a consequence of almost all profit generating crime, and therefore it can basically occur anywhere in the world. Generally, criminals tend to look for countries or sectors in which there is a low risk of detection. These countries usually have weak or ineffective AML programmes. Because the objective of money laundering is to get the illicit funds back to the criminal who gained them, launderers usually prefer to move the funds through stable financial systems. (FATF n.d..) Diane Francis, the author of the article "A Beginner's Guide to Laundering Money" (2014), states that according to UN, the largest recipient of Foreign Direct Investment (FDI) in 2013 was the British Virgin Islands, an archipelago with 23 000 residents. About $92 billion in foreign cash got washed up there. Other havens that received massive "investments" include Monaco and Cayman Islands. (Francis 2014.) Francis also states that the money doesn't necessarily stay where it gets washed, but is later on used for purchasing e.g. condos and other property in different countries.

The Basel Institute on Governance, a non-profit organization, creates annually a research-based ranking focusing on the risk of money laundering and terrorist financing. It is called the Basel AML Index, and it was first published in 2012. Altogether 14 indicators dealing with AML/CTF regulations, corruption, financial standards, political disclosure, and rule of law, are aggregated into one risk score. Since there are no quantitative data available, the Basel AML Index doesn't measure the actual existence of money laundering within a country, but rather indicates the risk level, the vulnerabilities so to say, of money laundering and terrorist financing within a country. The overall score is derived from indicators based on publicly available sources such as the FATF, the World Bank and Transparency International. The Basel AML Index is annually issued in two versions: the Expert Edition and the Public Edition. The Expert Edition provides a more comprehensive data set and serves as a tool for compliance officers. (The Basel Institute on Governance 2015, 1.)

The scores range from 0-10 where 0 indicates the lowest risk and 10 the highest risk (The Basel Institute on Governance 2015, 2). I won't go into further detail about the Basel Institute's methodology for calculating the overall score; the methodology is described in detail in the Basel AML Index 2015 Report. The map below shows the areas in the world where the risk levels are the highest.

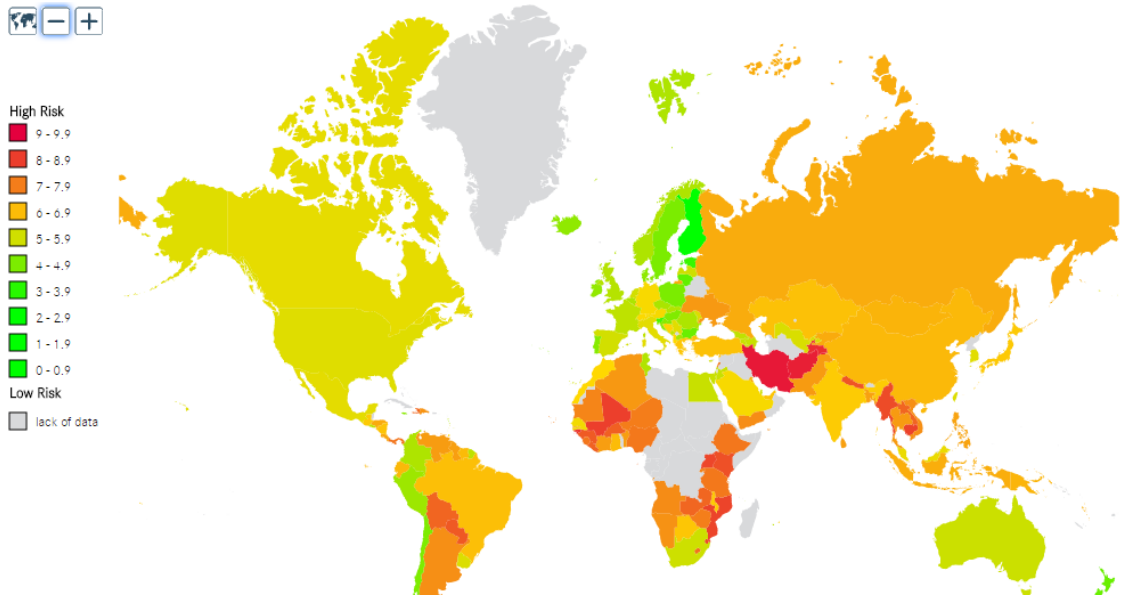

Figure 3. Country map (Basel Institute on Governance 2015).

The top five high-risk countries of the Basel AML Index 2015 risk rating are Iran, Afghanistan, Tajikistan, Guineau-Bissau, and Mali. More specifically, Iran is the highest risk country of the world with a score of 8.59. These high-risk countries are characterized by weaknesses in both preventing money laundering and terrorist financing, and enforcing multiple aspects of the AML/CFT framework. They also have structural and functional vulnerabilities such as high rates of perceived corruption, lack of resources to monitor the financial system, lack of judicial strength, and lack of public and financial transparency. (The Basel Institute on Governance 2015, 4.)

Finland, then again, is the lowest risk country with a score of 2.53. Estonia is the second lowest risk country with a score of 3.19. Finland and Estonia are the only countries that are below the risk threshold of 3.3, indicating a strong AML/CTF compliance level, low levels of corruption, and high financial and public transparency. (The Basel Institute on Governance 2015, 4.)

Also The FATF identifies jurisdictions that have strategic deficiencies in their AML/CTF procedures. (The FATF will be introduced in chapter 3.1.) The jurisdictions with most serious deficiencies are identified in two public documents that are issued three times a year. The FATF's last public statement was published in October 2015, stating that countries should apply counter-measures to Iran and the Democratic People's Republic of Korea. The FATF also called its members to consider the risks arising from the deficiencies associated with Myanmar. (FATF 2015.) Furthermore, the FATF identifies countries that have deficiencies in their AML/CTF measures, but who have developed action plans with the FATF to improve their AML/CTF regimes. However, I won't go into further detail about these countries.

To conclude, it can be said that developed countries are up to date with their AML/CTF measures, whereas developing countries have major deficiencies in their systems to combat money laundering and terrorist financing. Consistency with AML/CTF tools between different countries would be important in combating these crimes.

2.7 Money laundering in Finland

In Finland, the so called AML Act, which is better introduced later in this thesis, imposes an obligation on certain service providers, such as financial institutions, to monitor their customers' transactions and use of services. (Financial Supervisory Authority 2011). If these parties have suspicions of money laundering, they shall immediately report a suspicious transaction or a suspicion of terrorist financing to the Financial Intelligence Unit (FIU) (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Section 23). The FIU, which operates under the National Bureau of Investigation, has gathered information about the current state of AML/CTF actions in their annual report. In 2014, the FIU received 23 062 reports, which included 558 699 transactions. In the reporting system, it is possible to add several suspicious transactions to one report. (Krp 2014, 7-8.) The figure below shows the variety

of the reporting parties and the amount of reports each of them submitted to the FIU in 2014.

Table 1. Reporting parties (Krp 2014, 8).

Reporting parties	Reports in 2014
Banks	**1 125**
Investment firms	8
Other credit- and financial institutions	367
Insurance companies	156
Real estate businesses	10
Gaming operators	**9 100**
Payment service providers (including foreign exchange)	**12 092**
Accounting firms	11
Auditors	4
Advocates	4
Businesses dealing with valuable goods	89
Pawnshops	3
Management companies	2
Finnish police officers	2
Other Finnish authorities	82
Others	7
In total	**23 062**

The figure tells that money launderers prefer payment service providers, gaming operators and banks as intermediaries to transfer their illegally-gained funds. Payment service providers reported suspicions of money laundering most frequently: in 2014, they submitted 12 092 reports to the FIU.

In 2014, the FIU uncovered 44 new cases where pre-trial investigations were carried out later on. In addition to that, the FIU disclosed information to 246 cases where pre-trial investigations had already started earlier. In some cases, there were hundreds of reported transactions that supported the suspicion of money laundering. Almost all the reported cases were related to economic crimes. (Krp 2014, 13.) In Finland, most laundered money originates from economic crimes, whereas globally most originates from drug related crimes (Poliisi n.d.). In statistics, suspicious transactions are categorized into different

groups according to their nature. In the online reporting system, it is possible to choose one or more reasons for reporting the suspicion of money laundering. Therefore the amount of reasons that led to reporting is bigger than the amount of actual reports: 25 963 > 23 062. However, “the amount of money included in the transaction” was the most common reason to report suspicion of money laundering. (Krp 2014, 9.)

Table 2. Types of suspicious transactions (Krp 2014, 9).

Suspicious transaction	2014
Cash deposit	447
Cash withdrawal	263
Wire transfer	2 756
Capital recycling	304
Currency transfer	483
Currency exchange	45
Insurance	11
The amount of money included in the transaction	**17 712**
Sale of goods	93
Carrying cash	59
Other suspicious transaction	3 790
In total	**25 963**

The next statistics are interesting as they show the amounts of money, which involved suspicions of money laundering, that crossed the Finnish border in 2013 and 2014. The figures are based on the reports that the parties subject to the reporting obligation submitted to the FIU. In 2013, altogether almost 50 million euros, involving suspicions of money laundering, crossed the Finnish border. In 2013, there were suspicious money transfers from Finland worth around 33,6 million euros, whereas suspicious money transfers from abroad to Finland were worth around 15,5 million euros. (Krp 2014, 10.) What’s more interesting is how much the amount of incoming suspicious money increased in a year. In 2014, suspicious money transfers from abroad to Finland were worth around 330 million euros. Especially the amount of money transferred from

Europe and Asia increased enormously. (Krp 2014, 10.) I e-mailed the FIU to ask for the reason for this increase but they never got back to me.

Table 3. Money transfers from Finland abroad (Krp 2014, 10).

Money transfers from Finland abroad	2013 / €	2014 / €
Europe	17 918 587	21 349 401
Asia	7 842 405	8 367 070
Africa	6 064 216	6 142 339
America	1 665 541	1 047 797
Oceania	61 260	37 738
Unknown	42 346	1 153 063
In total	**33 594 355**	**38 097 408**

Table 4. Money transfers from abroad to Finland (Krp 2014, 10).

Money transfers from abroad to Finland	2013 / €	2014 / €
Europe	10 450 608	172 582 943
Asia	2 095 555	151 039 289
Africa	1 008 473	1 054 023
America	1 384 539	2 653 854
Oceania	177 978	174 675
Unknown	348 574	2 884 022
In total	**15 456 727**	**330 388 806**

3 MONEY LAUNDERING PREVENTION

Money laundering and terrorist financing are international issues. Various groups, accords, and treaties express a global focus on money laundering and how it is related to other crimes. Most nations see that permissive policies and structures can prompt criminal acts. The international community is nowadays willing to establish standards and codes of conduct relative to financial crime enforcement. Although the codes vary on the specific legal language, in general, they include guidelines on local, global, and multilateral cooperation, methods of capital flows across borders, record holding, requirements for customer identification and the description of suspicious transactions. Thus there has been an increase in cross-border coordination of investigations into corruption, misconduct, organized crime, and tracking the proceeds of crime in the global economy. (Turner 2011, 83.)

Many international instruments, including a number of international treaties, have been established to prevent and combat money laundering and terrorist financing. These treaties impose far-reaching obligations on individual states in international co-operation when it comes to preventing, combating and criminalizing money laundering and terrorist financing. Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (53/1994) is one example of these international instruments. In addition to Interpol and Europol, several international organizations are established to combat money laundering and terrorist financing. There is also “The Global Programme against Money Laundering” that operates under The United Nations Office of Drugs and Crime. (Poliisi n.d..) The Egmont Group, then again, is an informal network of Financial Intelligence Units (FIUs) established in 1995 to foster international co-operation. The group consists of more than 110 FIUs. (The Egmont Group n.d.; Poliisi n.d..) FIU.NET is a decentralized computer network created for the FIUs in the EU to enhance their collaboration (Poliisi n.d.). The Financial Action Task Force (FATF), then again,

is the most important international body to establish standards on AML and CTF measures.

The chart below shows how the international standards, and most importantly, the recommendations set by the FATF, form the basis for the EU's AML rules. Then again, the AML legislation in Finland is based on the EU Directive and the Regulation. The AML Act imposes an obligation on the parties subject to the reporting obligation inclunding banks, accountants, etc. The Financial Supervisory Authority ensures that the supervised entities meet the statutory requirements. Lastly, parties subject to the reporting obligation have to report a suspicious transaction or a suspicion of terrorist financing to the Financial Intelligence Unit. All these parties are introduced in the following sections.

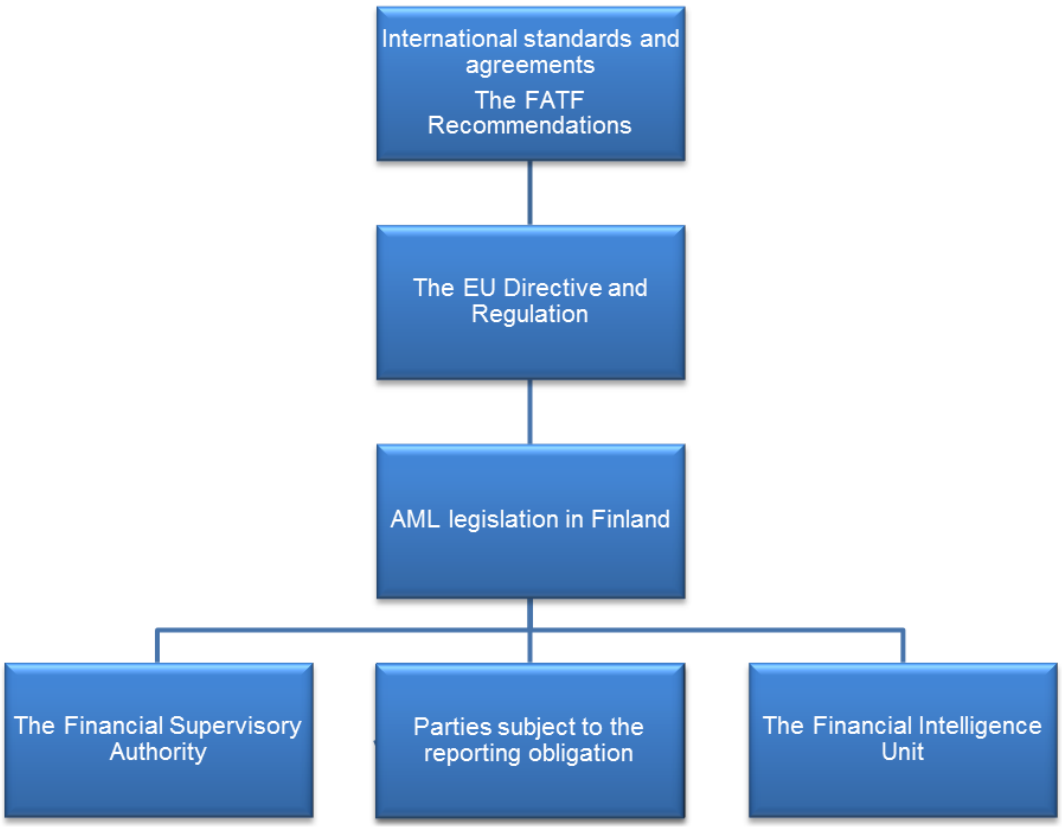

Figure 4. Interrelation between legislation and the ones the law applies to (Kuustie 2015).

3.1 The FATF

The Financial Action Task Force (FATF) was established in 1989 by the Ministers of its Member jurisdictions. It is an inter-governmental body whose objectives are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering as well as terrorist financing and other threats to the international financial system. Thus the FATF is a policy-making body whose aim is to generate the necessary political will to give rise to national legislative and regulatory reforms in these areas. The FATF currently comprises 34 member jurisdictions and 2 regional organizations, thus representing most major financial centres in all parts of the world. (FATF 2015.) The Presidency of the FATF is a one-year position held by a senior government official appointed from among the FATF members. He is supported by the FATF Secteriat which is located in the headquarters of the Organisation for Economic Co-operation and Development (OECD) in Paris. However, despite its location, the FATF is an independent body, and not part of the OECD. (Hopton 2009, 19.)

The FATF has created a series of recommendations on combating money laundering and financing of terrorism and profileration of weapons of mass destruction (FATF 2015). These Forty Recommendations form the basis of the most national laws on AML and CTF. After the terrorist attacks in the U.S. on September 11, 2001, the FATF expanded its mandate to incorporate efforts to combat terrorist financing by issuing an additional Nine Special Recommendations. (Hopton 2009, 19; FATF 2015.)

Since the FATF Recommendations were created in 1990, they have been adopted by over 190 countries. They are revised periodically, most recently in 2012, to make sure they are up to date and respond to current threaths to the financial system. In the most recent update of the Recommendations, the risk-based approach is emphasized more than in the previous versions. The risks are not the same for every country; however, the risk-based approach enables countries to devote their resources to the areas where the risks are the highest. (FATF 2015, 6.) Also, countries have diverse legal, administrative and

operational frameworks as well as different financial systems, and therefore they cannot all take the exact same measures to counter the threats. Thus the FATF Recommendations set an international standard which different countries need to apply through measures that are suitable for their unique circumstances. (FATF 2013, 7.) The FATF works in close co-operation with FATF-style regional bodies and the observer organizations, including e.g. the International Monetary Fund, the World Bank and the United Nations (UN). The FATF also maintains an active dialogue with the private sector and civil society. Thus the revised Recommendations has involved extensive consultation from these stakeholders. (FATF 2013, 8-9.)

The FATF Forty Recommendations are divided under the following 7 titles:

A. AML/CTF policies and coordination

B. Money laundering and confiscation

C. Terrorist financing and financing of proliferation

D. Preventive measures

E. Transparency and beneficial ownership of legal persons and arrangements

F. Powers and responsibilities of competent authorities, and other institutional measures

G. International Cooperation

(FATF 2013, 11-30.)

By publishing monitoring reports, the FATF assesses the member countries' legislation and the actions taken by public authorities against the Recommendations. Also, as stated earlier, the FATF peridiocally identifies juridictions that have strategic deficiencies in AML and/or CTF measures. (Sisäministeriö 2015.)

3.2 The EU Directive and Regulation

The EU rules in the area of combating money laundering and financing of terrorism are largely based on international standards created by the FATF. They are tailored to the EU's needs and complemented by national provisions. (European Commission 2015.) The following provisions are in force in the EU:

- Directive (EU) 2015/849 on preventing the use of the financial system for money laundering or terrorist financing (4th Anti-Money Laundering Directive)
- Regulation (EU) 2015/847 on information on the payer accompanying transfers of funds

The EU Directive 2015/849 seeks to protect credit and financial institutions against the risks of money laundering and terrorist financing, whereas the EU Regulation 2015/847 is aimed to make fund transfers more transparent. (European Commission 2015.) The EU Directive 2015/849 came into force on 20 May 2015, "amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC" (European Union 2015). According to the Directive (EU) 2015/849, Article 67: "Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 26 June 2017. They shall immediately communicate the text of those measures to the Commission."

The Directive primaly applies to the financial sector including banks, accountants, trust or company service providers, accountants and lawyers. Also, any other kinds of businesses involved in making or receiving cash payments for goods worth at least 10.000€ have to comply with the rules, regardless of whether payment is made in single or more linked transactions. (Out-Law 2015; Chave et al. 2015, 1-2.)

The key Directive requirements are Customer Due Diligence, record-keeping, suspicious-transaction reporting and internal controls. The previous Directive had the same elements; however, the 4th Directive brought some changes to the previous one. The new regime brought into force new Customer Due Diligence checking requirements: Simplified Due Diligence was made more complex whereas Enhanced Due Diligence now applies also to domestic Politically Exposed Persons (PEPs) (Chave et al. 2015, 2). I will better introduce these concepts later on. An other important change is that all member states will need to introduce an "ultimate beneficial owner" register, where officials have an access to. Central registers will enable greater transparency in financial transitions. (Out-Law 2015.) The new Directive increases senior managers' responsibilities in recognizing money laundering attempts. Also, sanctions for non-compliance will increase significantly. (Chave et al. 2015, 2.)

The Regulation (EU) 2015/847, then again, is binding in its entirety and is directly applicable to all Member Sates. The Regulation will apply from 26 June 2017. (Regulation (EU) 2015/847 of the European parliament and of the council, Article 27.) The previous regulation on information on the payer accompanying transfers of funds 1781/2006 will be repealed.

The Regulation seeks to improve the traceability of payments and information on the payer and the payee in order to detect money laundering and terrorist financing. In short, it can be said that the Regulation applies if there is at least one payment service provider (PSP) involved in the transfer, which is established in the Union. The PSP of the payer needs to ensure that transfers of funds are accompanied by the following information *on the payer*: the name of the payer, the payer's payment account number, and the payer's address, official personal document number, customer identification number or date and place of birth. Also, the PSP of the payer needs to ensure that transfers of funds are accompanied by the following information *on the payee*: the name of the payee, and the payee's payment account number. The information on the payer and the payee has to be retained for 5 years after the transfer of funds. (OPF-Partners 2015.) There are some exception to the Regulation, as well as other

important points to complying with it but I won't go into further details about them.

Finland will have to adjust its laws and regulations to comply with the new Directive and the Regulation by 26 June 2017. At the moment, the Finnish AML legislation complies with the previous EU Directive. The parties that the Directive and the Regulation applies to should start preparing themselves well in advance so that their operations are up to date when the Directive and the Regulation are actually implemented into Finnish legislation.

3.3 Legislation in Finland

In Finland, money laundering became a punishable offence in 1994. Before the EU provisions on money laundering came into force, there had been no uniform legislation in Finland to prevent and investigate money laundering. (European Commission 2006; Poliisi n.d..) The criminal sentence depends on whether the perpetrator has himself committed the predicate offence or has only got involved in the money laundering. In Finland, the predicate offence may be any committed crime, as long as it has brought economic benefit to the perpetrator. If the money launderer has himself committed the predicate offence, he will only be punished for that crime. If the person has not been involved in committing the predicate offence, but has only been involved in the money laundering, he will be sentenced for money laundering under sections 6-10 of the Criminal Code of Finland (Poliisi n.d.).

However, if a person has himself committed the predicate offence, he may still be sentenced for aggravated money laundering if "the money laundering offence, with consideration to the continuous and planned nature of the acts forms the most essential and blameworthy part of the totality of offences" (the Criminal Code of Finland 39/1889, Section 11). This is because in some cases the punishment for money laundering is tougher than the punishment for the predicate offence would be. Thus this provision prevents criminals from "tricking" with the punishments.

3.3.1 Money laundering as a criminal offence

The Criminal Code of Finland (39/1889, Section 6) defines the crime of money laundering as following:

(1) A person who

1. receives, uses, converts, conveys, transfers or transmits or possesses property acquired through an offence, the proceeds of crime or property replacing such property in order to obtain benefit for himself or herself or for another or to conceal or obliterate the illegal origin of such proceeds or property in order to assist the offender in evading the legal consequences of the offece or
2. conceals or obliterates the true nature, origin, location or disposition of, or rights to, property acquired through an offence, the proceeds of an offence or property replacing such property or assists another in such concealment or obliteration,

shall be sentenced for *money laundering* to a fine or to imprisonment for at most two years.

(2) An attempt is punishable.

(Criminal Code of Finland 39/1889).

In the Criminal Code of Finland (39/1889, Chaper 32 Sections 6-10), money laundering is divided into following sections: *money laundering, aggravated money laundering, conspiracy for the commission of aggravated money laundering, negligent money laundering* and *money laundering violation*. Money laundering is considered to be aggravated if the property acquired through the offence has been very valuable or the crime is committed in a particularly intentional manner. In the case of *aggravated money laundering*, the offender shall be sentenced to imprisonment for at least four months and at most six years. Here an attempt is also punishable. A person can be sentenced for *conspiracy for the commission of aggravated money laundering* if he or she

agrees with another on the commission of aggravated money laundering directed at the proceeds of the giving of a bribe, the acceptance of a bribe, or aggravated tax fraud or aggravated subsidy fraud directed at the tax, or at property replacing such proceeds. The sentence for this offence is a fine or an imprisonment of at most one year. Then again, a person who through gross negligence launders money, shall be sentenced for *negligent money laundering* to a fine or to imprisonment for at most two years. Lastly, if the money laundering or the negligent money laundering is petty when assessed as a whole, the offender shall be sentenced for a *money laundering violation* to only a fine. (Criminal Code of Finland 39/1889 Sections 6-10; Talousrikos n.d..)

3.3.2 Confiscation

Organized crime activities are mostly profit driven. The confiscation of the proceeds of crime deprive criminals of what they have worked hard to acquire. Confiscation has a deterrent effect as it prevents criminals from benefiting from the proceeds of crime. When the criminal forfeits the illicit funds, he/she may not use them to finance new crimes. It is said that when the criminal forfeits the economic benefit gained from the crime, it will decrease his/her motivation to commit new crimes. (Sahavirta 2008, 363 – 365; European Commission 2015.)

In the Criminal Code of Finland, it is stated that the property that has been the target of money laundering, aggravated money laundering or negligent money laundering, shall be ordered forfeit to the State. However, the property that is the target of the offence may, instead of being ordered forfeit to the State, be ordered as compensation or restitution to the person injured by the predicate offence, if the nature of the property is suitable for this, and compensation or restitution has not already been paid to him or her. If the nature of the property is not suitable to be paid as compensation to the injured person, it shall be ordered forfeit, and the injured person has the right to receive a comparable amount as compensation or restitution from the State funds. (Criminal Code of Finland 39/1889, Section 12.)

According to European Commission, the current number of freezing and confiscation procedures in the EU and the amount of proceeds recovered from organised crime seem modest if compared to the estimated revenues of these criminals. (European Commission 2015). Therefore it is important to enchance the international cooperation in tracing criminal assets, so that they can be ordered forfeit.

3.3.3 Anti-money laundering legislation in Finland

The Act on Detecting and Preventing Money Laundering and Terrorist Financing, the so called AML Act, became effective on 1 August 2008. The Act is supplemented by Government Decrees 616/2008 and 1204/2011, Decision by the Ministry of the Interior 156/2010 and Government Decision 1022/2010. The AML Act based on the EU's Third Anti-Money Laundering Directive. (Financial Supervisory Authority 2014.) The purpose of the AML Act is to prevent money laundering and terrorist financing, to promote the detection and investigation of them and to reinforce the tracing and recovery of the proceeds of crime. Shortly, the AML Act applies to banks, advocates, investment firms, management companies, insurance companies, gaming operators, auditors, and businesses or professions dealing in goods to the extent that payments are made in cash in an amount of 15.000 euros or more. (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Sections 1-2.) The new EU Directive that was discussed earlier will lower that amount to 10.000 euros. The AML Act also applies to branches of foreign credit institutions, insurance companies, investment firms etc.

The key principles of the AML Act are Customer Due Diligence and a risk-based approach to money laundering and terrorist financing. CDD means the procedures related to customer identification, knowing one's customer, and ongoing monitoring. CDD enables the service provider to ascertain the real identity of the customer and to have an adequate knowledge of the customer's business. A risk-based assessment means that service providers have internal operational methods and processes in place, adequate with the nature and size

of their operations, for assessing the risks of money laundering and terrorist financing related to their customers, services and products. Service providers need to review their customer relationships, services, products and distribution channels, and assess whether CDD measures are as adequate as required in the law. If necessary, service providers have to update their previous information on customers. The Act requires the parties subject to the reporting obligation, for example, to identify the beneficial owner and to clarify corporate customers' ownership structures: the natural persons whose ownership of holdings or controlling interests exceeds 25% need to be identified. (Financial Supervisory Authority 2011.)

If there is a higher risk of money laundering or terrorist financing, the risk-based approach requires particular care in measures taken for CDD. This *enhanced Customer Due Diligence* means obtaining more information on the customer's business and closer monitoring of the relationship than normally. On the other hand, if there is a lower risk of money laundering and terrorist financing, the measures taken for customer due diligence may be more limited. This is procedure is called a *simplified Customer Due Diligence.* (Financial Supervisory Authority 2011.)

The AML Act imposes an obligation on above mentioned service providers to monitor customer relationships, use of services and transactions on a regular basis throughout the existence of the customer relationship (Financial Supervisory Authority 2011). According to the Act on Detecting and Preventing Money Laundering and Terrorist Financing (503/2008, Section 9) "Parties subject to the reporting obligation shall pay particular attention to transactions which are unusual in respect of their structure or extent or the size or office of the parties subject to the reporting obligation. The same also applies if transactions have no apparent economic purpose or if they are inconsistent with the parties' experience or knowledge of the customers. If necessary, measures shall be taken to establish the source of funds that are involved in a transaction." For example, if a customer wishes to deposit a large sum of cash to his/her account, he/she may be asked for a document to prove the origin of

that cash money. If suspicions are to arise, parties subject to the reporting obligation shall immediately report a suspicious transaction or a suspicion of terrorist financing to the Financial Intelligence Unit. Parties subject to the reporting obligation shall suspend a transaction for further inquiries or refuse to conduct a transaction if the transaction is either suspicious or they suspect that the funds involved in the transaction are used for terrorist financing or a punishable attempt to finance terrorism. (The Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Sections 23-26.)

According to the Act on Detecting and Preventing Money Laundering and Terrorist Financing (503/2008, Section 40), anyone who deliberately or through negligence fails to fulfil the obligation to conduct CDD, or the obligation to keep records of the CDD data, shall be sentenced for *violation of customer due diligence* to a fine.

The Ministry of Finance set up a working group in December 2014 to prepare a prosal for a new AML Act that complies with the EU's fourth Anti-Money Laundering Directive and the FATF's 40 Recommendations. One of the goals for the working group is also to assess the penalty system and the supervisory structures of money laundering and terrorist financing. (Krp 2014, 4.)

3.3.4 The acts and decrees that are in force in Finland

In Finland, the Ministry of the Interior is responsible for the development of AML legislation. Some of the acts and decrees are available only in Finnish and in Swedish. The following acts and decrees are currently in force in Finland:

- Act on Detecting and Preventing Money Laundering and Terrorist Financing (503/2008)
- Government Decree on Preventing and Clearing Money Laundering and Terrorist Financing (616/2008)

- Government Decree on simplified customer due diligence related to certain financial contracts in the prevention and detection of money laundering and terrorist financing (1204/2011)
- Ministry of the Interior Decision on non-EEA states and territories whose provisions on preventing and detecting money laundering and terrorist financing meet the requirements laid down in the Act on Preventing and Detecting Money Laundering and Terrorist Financing (156/2012)
- Government Decision on states and territories whose provisions on preventing and detecting money laundering and terrorist financing do not comply with the international requirements laid down in the Act on Preventing and Detecting Money Laundering and Terrorist Financing (1022/2010)
- The Criminal Code (39/1889)
    - Chapter 32 (Receiving and money laundering offences)
    - Chapter 34 a (Terrorist offences)
    - Chapter 46 (Regulation offences and smuggling)
- Credit Institutions Act, section 145 (121/2007)
- Investment Firms Act, section 69 (922/2007)
- Act on amendment of section 144 on Mutual Funds Act (507/2008)
- Act on the Book Entry System, section 29 b (826/1991)
- Act on Payment Institutions, section 39 (297/2010)
- Decree by the Ministry of Finance on information to be attached to authorisation applications by credit institutions, section 16 (939/2007)
- Decree by the Ministry of Finance on information to be attached to authorisation applications by investment firms, section 12 (937/2007)

- Decree by the Ministry of Finance on information to be attached to authorisation applications by fund management companies and custodians, section 12 (938/2007)
- Ministry of Finance Decree on the information to be appended to the authorisation application of a payment institution (554/2011) (Financial Supervisory Authority 2012.)

3.4 The Financial Intelligence Unit

In Finland, the Financial Intelligence Unit (FIU) operating under the National Bureau of Investigation deals with reports submitted to them on suspicious transactions (Financial Supervisory Authority 2014). The FIU was established in 1998 (Poliisi n.d.). According to the Act on Detecting and Preventing Money Laundering and Terrorist Financing (503/2008, Section 35) the duties of the FIU are following:

- detecting and preventing money laundering and terrorist financing by receiving, recording and examining reports on suspicions of money laundering and terrorist financing as well as investigating crimes that were committed to gain the proceeds of crime subject to money laundering and terrorist financing
- promoting cooperation between authorities in the fight against money laundering and terrorist financing
- cooperation and exchange of information with the authorities of a foreign state and international organizations that are responsible for detecting and preventing money laundering and terrorist financing
- cooperation with the parties subject to the reporting obligation
- giving feedback on the effects of submitted reports
- keeping statistics on the number of reports received and the number of transactions suspended

The National Bureau of Investigation is also obliged to provide the National Police Board with an annual report on the activities of the FIU and the progress of AML and CTF actions in Finland in general. (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Section 35; Poliisi n.d..)

The operations of the FIU are divided into three divisions. The division that receives reports on suspicious transactions analyzes and registers them. The investigations division then carries out an initial investigation and determines whether a pre-trial investigation needs to be conducted. The division of international affairs, then again, takes care of international inquiries and contacts, and deals with the CTF issues. (Poliisi n.d..)

Parties subject to the reporting obligation have to report a suspicious transaction or a suspicion of terrorist financing to the FIU via online reporting system. The link to the system can be found on the webpage of the National Bureau of Investigation. Both organization representatives and individual persons have to register themselves into the system before they are able to report a suspicion (Poliisi n.d.).

3.5 The Financial Supervisory Authority

The Finnish Financial Supervisory Authority (FIN-FSA) supervises Finland's financial and insurance sectors. The entitites supervised by the FIN-FSA include banks, insurance and pension companies as well as other companies operating in the insurance sector, fund management companies, investment firms and the Helsinki stock exchange. 95% of the activities of the FIN-FSA is funded by the supervised entitites and the remainder is provided by the Bank of Finland. Although FIN-FSA operates in connection with the Bank of Finland, it makes independent decisions in their supervisory work. (Financial Supervisory Authority 2015.)

When it comes to combating money laundering and terrorist financing, the FIN-FSA is responsible for ensuring that the procedures, risk management and internal control of supervised entities meet the statutory requirements. If a

supervised entity or its employee fails to comply with the obligations of customer due diligence, they may be sentenced to a punishment. A supervised entity may become guilty of negligent money laundering if it assists or counsels a customer in connection with, for example, investment activities or transfer of funds, although there are weighty reasons to be suspicious of the customer's business. (Financial Supervisory Authority 2014.) The administrative sanctions and supervisory measures exercised by the FIN-FSA are following: a temporary prohibition from holding a managerial position in a supervised entity, a curtailment of operations subject to authorization, administrative fines, public warnings, and penalty payments. The harshest punishment for non-compliance with the obligations is the penalty payment. The size of the penalty payment is based on a comprehensive assessment: consideration is given, for example, to the nature, scope and duration of the breach. The maximum penalty for a legal person - a business entity - is 10% of the consolidated financial statements, while that for a natural person is 5 million euros. (Financial Supervisory Authority 2015.)

In May 2015, Sweden's Financial Supervisory Authority fined banking groups Nordea and Handelsbanken for non-compliance with the AML and CTF legislation. Nordea, the Nordic region's biggest financial services group, was fined 50 million SEK, which is approximately 5,4 million euros, for having major deficiencies in its approach to tackling money laundering. According to the FSA, Nordea had lacked an effective system to detect and prevent money laundering for several years, whether identifying high-risk individuals, suspicious transactions and counterparts in tax havens or countries linked to terrorism. The severity of the non-compliance would have even justified revoking Nordea's banking license, but because Nordea had already taken measures to address the problems, the FSA only issued a warning alongside the fine. Handelsbanken, then again, was fined 35 million SEK, which is approximately 3,7 million euros. Handelsbanken got only a remark, which is a less serious official sanction than a warning. (Reuters 2015; Kervinen 2015.) After getting fines this big, the banks probably don't want to risk their businesses anymore by

having deficiencies in their measures to combat money laundering and terrorist financing.

4 THE ROLE OF A BANK

In this chapter, the Finnish AML Act that was discussed in chapter 3.3.3 is looked more deeply into. Banks in Finland are obliged by the Act on Detecting and Preventing Money Laundering and Terrorist Financing to know their customers, monitor their customer relationships and customers' transactions, and to report suspicious transactions to the Financial Intelligence Unit. Banks must have such risk management procedures in place that are commensurate with the nature and size of their business. In this chapter, I will go through the key principles of the AML Act that affect the operations of banks.

I interviewed the service manager of a bank in Finland to get an insight how the law is applied in practice. He wished that I would not mention the name of the bank, and therefore I will refer to ”Bank X”. When talking about the service manager, I will refer to ”Mr Y”. The interview questions were sent to the service manager one week prior to the interview. The interview was conducted in Finnish, and thus the questions sent beforehand are in Finnish. They can be found in the Appendix 1. The questions go hand in hand with the Finnish AML Act: I first introduce a law section and then get a practical view by deploying the interview answers. I first tried to get an interview from the bank where I worked in the summer, but they did not agree to give any information. Therefore I approached the service manager of Bank X. He's an expert in the AML field and has a vast knowledge on complying with the AML law. Unfortunately he was not allowed to give very detailed information to be published, though. Gaining primary qualitative data for this thesis was thus a challenge, in deed. In addition to the interview, I reflect my own observations from my experience working as a cashier service officer. My own observation are part of the empirical part.

Note: The AML Act applies to all ”parties subject to the reporting obligation”, such as insurance companies and auditors, but in this chapter I will only refer to banks.

4.1 Risk based approach

As said, banks need to have in place such risk management procedures related to money laundering and terrorist financing that are commensurate with the size and nature of their operations. When assessing the risks of money laundering and terrorist financing, banks have to take into account the risks that are related to their sector, products, services, customers, the customers' business and transactions, as well as to technological development. The CDD measures need to be observed on the basis of risk-based assessment throughout the existence of the customer relationship. Banks need to show the Financial Supervisory Authority that their methods for CDD and ongoing monitoring are adequate and comply with the AML Act. (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Section 6.) The risk assessment can be used for classifying the customers into different groups based on the level of risk they present. Risk assessment needs to be reviewed on a regular basis and updated when necessary. (Financial Supervisory Authority 2010, 14-16.)

I asked Mr Y what kind of risk assessment Bank X uses, but he could not give an exact answer. He said that Bank X "acts according to the recommendations given by the Federation of Finnish Financial Services", and that "Bank X does its risk assessment based on those recommendations". He said that risk assessment involves both technology and people. When I asked what kind of risk categories customers are divided into, Mr Y could not answer at all. (Mr Y, interview 11.11.2015.)

According to the Financial Supervisory Authority (2010, 16), banks' should have effective risk management systems in place. Bank X belongs to a financial group, and the risk management guidelines come from the group level. The group that Bank X belongs to has a risk management department including a compliace unit. They give the instructions to the banks belonging to the group. Bank X acts according to these instructions. However, Bank X has also a risk management unit of its own. The compliance with the agreed principles is

ensured by internal control and supervisory. The compliance is also documented. (Mr Y, interview 11.11.2015.)

4.2 CDD - Customer Due Diligence

CDD obliges banks to know their customers. According to the AML Act, banks need to identify their customers and verify their identities in certain situations. Identification means establishing the customer's identity on the basis of information provided by the customer; whereas verification of the identity means ascertaining the customer's identity on the basis of documents, data or information obtained from a reliable and independent source. According to the AML Act, banks need to identify the customer and verify the customer's identity when:

- establishing regular customer relationships;
- in case of suspicious transaction or if they have a suspicion that the funds involved are used for terrorist financing;
- when they have doubts about the reliability of previously obtained data on the customer's identity;
- if someone acts on the behalf of the customer, the representative must be identified, and his/her identity must be verified if necessary;
- when the sum of a transaction is 15,000€ or more, regardless of whether payment is made in single or more linked transactions, and when the customer relationship is not regular. (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Sections 5 - 7; Financial Supervisory Auhtority 2010, 18-19.)

However, banks are obliged by the Payer Information Regulation (1781/2006) to identify and verify the customer's identity when the amount of the transfer of funds, that is conducted in cash, exceeds 1000€ (Financial Supervisory Authority 2010, 19). This means that if a customer wishes to deposit 1000€ in cash even into his/her own bank account, he/she must be identified (Financial

Supervisory Authority 2010, 35). Banks may apply stricter internal instructions, too. For example, when I worked as a cashier service officer in the summer of 2015 in a bank, we always verified the customer's identity, even if they deposited less than 1000€ to their account. Also, if they wanted to pay invoices in cash, no matter what the amount of funds involved was, we always verified the customer's identity. The Payer Information Regulation obliges banks to make sure that transfers of funds are accompanied by the following information on the payer: the name of the payer, the payer's payment account number, and the payer's address, official personal document number, customer identification number or date and place of birth. The aim of the regulation is to ensure that officials are able to trace suspicious transfers. (Financial Supervisory Authority 2010, 35.) The new EU regulation on information on the payer accompanying transfers of funds (2015/847), which was introduced in chapter 3.2, will apply from 26 June 2017, repealing the previous regulation (1781/2006). (Regulation (EU) 2015/847 on information on the payer accompanying transfers of funds, Article 26.)

When the customer is present in person, his/her identity needs to verified on the basis of an official document. The identity documents that are considered reliable for banking purposes in Finland, providing that they are in force and issued by a Finnish authority, are:

- Passport
- Identity card (also temporary)
- Driving licence
- Photo-bearing identity card issued by the Social Insurance Institution of Finland
- Alien's passport
- Diplomatic passport
- Refugee's travel document

Then again, valid passport is the only foreign-issued document accepted as a reliable proof of identity. However, identification cards used in the EU and EEA as travel documents may also be accepted as proof of identity at banks if their authenticity can be verified. (Federation on Finnish Financial Services n.d..) However, on the basis of its own risk management principles, the bank may decide which documents to accept for verification purposes. In the case where the customer relationship is established without having the customer physically present, for example in an online service, the customer's identity can be verified by, for example, using an electronic identification device that fulfils the criteria of strong electronic identification device, such as an online banking code or a mobile certificate. (Financial Supervisory Authority 2015.)

Banks also need to identify the beneficial owners, and if necessary, verify their identity (Act on Detecting and Preventing Money Laundering and Terrorist Financing, Section 8). Beneficial owner means a natural person on whose behalf the transaction is being conducted, or if the customer is e.g. a company, it means the natural person who controls the company. A natural person is deemed to exercise control when his/her ownership of holdings or controlling interests exceeds 25%. (Financial Supervisory Authority 2011.) However, according to the AML Act, there are situations where beneficial owners do not have to be identified. An example of that kind of situation is when the customer is a company or corporation whose securities are admitted to public trading referred to in the Securities Markets Act or to similar trading in another EEA State. There are also other situations where the beneficial owner does not have to be identified but I won't go into further detail about them.

By identifying the customer it is meant that banks must have sufficient information on their customers' activities, financial status, banking practices, and purpose for which the services are used. Banks need to find out what kind of services their customers need. Furthermore, the law requires banks to ask where their customers' incoming money comes from and what the money is going to be used for. A bank can for example request a written clarification from its customer on the origin of funds paid to the customer's account. Also, if a

customer wishes to deposit what a bank considers to be a large amount of cash into his/her account, he/she may be asked for a document that proves the origin of that money, such as a bill of sale. (Federation of Finnish Financial Services n.d.; Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Section 9; Financial Supervisory Authority 2015.) These questions may irritate customers as they are perceived as too personal. Thus it is important to tell the customers that the bank has the statutory obligation to know their customers. On the other hand, customers are used to answer questions concerning their personal expenditure and income as banks need this information to make mortgage decisions. However, questions concerning the customer's political influence may cause bewilderment among customers. (Federation of Finnish Financial Services 2015.)

I asked Mr Y what kind of questions are asked in Bank X when establishing a new customer relationship. According to him, no matter whether the customer is a personal customer or a corporate customer, all the information that is required by the law for CDD is asked. "When it comes to personal customers, it is a bit more simple. When establishing a customer relationship with a corporation, we have to find out the business structure and type, as well as the company background. Then we get to the point where we have to identify the beneficial owner" (Mr Y, interview 11.11.2015). Basic information is updated in every customer meeting, regardless of the channel (Mr Y, interview 11.11.2015).

According to Uusi Suomi (2015), customers have been disconcerted by the detailed questions that banks have been asking them. I asked Mr Y how the customers of Bank X react to the questions about their incoming money, political influence and so on. He said that they take the questions mainly well, although there are some exceptions. "In my opinion, it has changed during the past half year. It has been talked about a lot recently and thus the customers' attitude has changed." Mr Y stated that there used to be customers who didn't quite understand the reasoning behind the questions and got irritated, but nowadays that kind of behavior has basically disappeared. The customers are always told why the bank asks such questions. The Bank X has also a written

document that they can hand out to the customer in case he/she wishes to see some facts why such questions are asked. (Mr Y, interview 11.11.2015.)

Finland and the US have agreed on information exchange subject to FATCA, Foreign Account Tax Compliance Act concerning the taxation of U.S. foreign accounts. Due to the agreement, banks must yearly recognize the accounts and assets of U.S. persons and report their number and amount of assets to Finnish Tax Administration. Finnish Tax Administartion will then report the information further to the U.S. tax authority, the Internal Revenue Service. (Verohallinto 2015.) The aim of the FATCA agreement is to prevent tax evasion of U.S. citizens (Federation of Finnish Financial Services 2014). That's why banks' customers are also asked if they have connections to the U.S..

4.3 CDD data and record keeping

Banks have to document the customer identification and due diligence information. Records have to be retained in a secure manner for five years following the end of regular customer relationship. When the transaction is occasional amounting to over 15,000€, the records need to be kept for five years following the carrying-out of the transaction. The following information must be retained:

- name, date of birth and personal identity number
- name, date of birth and personal identity number for someone acting as a representative
- full name, register number, register date and registering authority for a legal person
- full name, date of birth and nationality of the member of the board or an equivalent decision-making body of a legal person
- business sector of the legal person
- name, date of birth and personal identity number of beneficial owner

- name, number or other identifier and issuer of the document used in the verification of identity, or a copy of the document
- the information that is necessary to conduct customer due diligence, such as information on the customer's transactions, the nature and extent of the customer's business, his/her financial status, the grounds for the use of transactions or services and information on the source of funds

If the customer is a foreigner without a Finnish identity code, records need to be retained of the customer's citizenship and travel document in addition to the above mentioned data. (Act on Detecting and Preventing Money Laudering and Terrorist Financing 503/2008, Section 10; Financial Supervisory Authority 2015.)

The above mentioned data has to be retained so that banks can later, if necessary, demonstrate to officials how each customer has been identified, which document was used for verifying the customer's identity and who conducted the CDD measures. The customer has the right to access his/her identification information. However, banks may not disclose the making of a suspicious transaction report to the customer subject to the suspicion. Thus the data necessary to fulfil the reporting obligation has to be kept separate from the customer register. Customers don't have an access to this information. (Financial Supervisory Authority 2010, 33.)

4.4 Enhanced vs. Simplified CDD

According to the AML Act, banks must apply enhanced CDD measures in situations where the customer, service, product, or transaction represents a higher risk of money laundering or terrorist financing, or where the customer or the transaction is connected with a state whose system of detecting and preventing money laundering and terrorist financing doesn't meet the international standards. (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Section 17.) In practice, enhanced CDD

means that the documentation of the customer's transactions needs to be done even more carefully, and the customers who are subject to enhanced CDD measures need to be observed more carefully in ongoing monitoring. Banks have to apply enhanced CDD measures to customers who are in connection with high-risk countries. By connection it is meant, for example, that the customer's home country is one of the high-risk countries, or that he/she does business with a company from one these countries. (Financial Supervisory Authority 2010, 27.) Different bodies identify countries that have strategic deficiencies in their AML/CTF procedures. As discussed earlier, the FATF and the Basel Institute on Governance are examples of those who list high-risk jurisdictions. I asked Mr Y whether he knew whose listing Bank X uses. According to him, Bank X uses the so called FATCA list but he didn't know who has drawn it up. (Mr Y, interview 11.11.2015.)

If the customer is not physically present when he/she is identified and his/her identity is verified, banks need to take additional measures to reduce the risk of money laundering and terrorist financing. They can, for example, verify the customer's identity on the basis of additional documents obtained from a reliable source, or verify his/her identity by means of verifiable electronic identification, such as an online banking code. (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Section 18; Financial Supervisory Authority 2010, 28.)

Enhanced CDD measures must be applied also when the bank concludes a contract on the handling of payments and other assignments with a credit institution located in a country outside the EEA. In this case, the bank has to obtain sufficient information about the respondent institution before concluding the contract. For example, the bank has to assess the respondent credit institution's reputation and its AML and CTF measures. Also, if the respondent credit institution is subject to the UN's or the EU's financial sanctions, the bank can not start a correspondent banking relationship with it. (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Section 19; Financial Supervisory Authority 2010, 29.) The bank can neither start a banking

relationship with a so called shell bank that is located in a tax haven (Financial Supervisory Authority 2010, 29).

When obtaining information about customers, the bank has to determine whether the customer is holding, or has held, an important public position in another state. This is related to enhanced CDD, because it is considered that politically exposed persons (PEPs) are prone to corruption, and thus bear higher risk of becoming involved in money laundering. Enhanced CDD applies to the PEP's family members and close associates, too. Positions that are considered to be prominent public functions are held by presidents, ministers, ambassadors, etc.. (Krp 2012, 34-35.) As there is no register of PEPs, banks are forced to ask their customers whether they are politically exposed. This is perceived as awkward among both the customers and the bank employees. (Federation of Finnish Financial Services 2013.) However, it might be rather difficult to maintain such register, as "a person is no longer considered a politically exposed person when he or she has not held an important public position for at least one year" (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Section 20). Thus the list of PEPs would be changing all the time. The register would also have to include PEPs' family members which would increase the difficulty to create such register. As said, the customer is considered as a PEP only if he/she is holding, or has held, an important position in another state. However, the EU's 4th AML Directive brought into force new customer due diligence checking requirements where enhanced CDD will apply also to domestic PEPs. The new directive has to be implemented into Finnish legislation by 26 June 2017 (EU Directive 2015/849, Section 67).

In case it is determined that a customer is a PEP, the senior management of the bank has to give its approval for establishing a customer relationship with such person. Also, the bank needs to establish the source of wealth and funds that are involved in that customer relationship or transaction. Enhanced ongoing monitoring of the customer relationship needs to be conducted, too. (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008.)

Whereas enhanced CDD measures need to be applied when the customer or the transaction represents a higher risk of money laundering or terrorist financing, simplified CDD measures can be applied when the customer, product, or transaction represents a low risk of money laundering and terrorist financing. Simplified CDD measures can be applied if the customer is e.g. a Finnish authority; a credit institution, a financial institution, or an investment firm that is duly authorised in Finland or in another EEA State. Simplified CDD measures may also be applied if one of the above-mentioned is located in a non-EEA State that is subject to the obligations equivalent to those in the Finnish AML Act. The bank may also apply simplified CDD measures if the customer is a company whose securities are admitted to public trading. (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Sections 13-14.) By products that represent a low risk of money laundering it is meant certain insurance products (Financial Supervisory Authority 2010, 31-32).

In practice, applying simplified CDD measures means that the bank doesn't have to identify the beneficial owner and doesn't have to clarify the company structure. Neither do the bank have to obtain the amount of information that it would normally have to. However, the identity of the company repsentative must still be identified. Also, despite applying simplified CDD measures, the bank must still monitor the customer relationship in order to detect any exceptional or unusual patterns of transactions. (Krp 2012, 29-30.) It can be said that simplified CDD measures can not be applied to "normal customers" even if they don't represent necessarily a higher risk of money laundering or terrorist financing.

4.5 Ongoing monitoring

According to the AML Act, banks are obliged to arrange monitoring that is adequate in the view of the nature, extent and risks of the customers' transactions to ensure that the transactions are consistent with the banks' experience or knowledge of the customers and their business. Banks must pay particular attention to transactions which are unusual in respect of their

structure, quantity or size. The same also applies if transactions have no apparent economic purpose or if they are inconsistent with the banks' experience or knowledge of the customers. If necessary, measures need to be taken to establish the source of funds that are involved in the unusual transaction. (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Section 9.)

Banks need to have enough resources to arrange ongoing monitoring. They should also have in place internal instructions for using the monitoring system. As the AML Act applies to a variety of businesses, there is no definite requirements for monitoring systems. Thus each bank may have a different type of monitoring system. The monitoring system may be automated or manual, or a combination of these two, as long as it is adequate for meeting the requirements of detecting unusual transactions. (Financial Supervisory Authority 2010, 34.)

I asked Mr Y how Bank X has organized ongoing monitoring and how they detect unusual transactions. He could not give an exact answer as he only stated that they "react to deviations regardless of the channel". As said, the process involves both technology and people. I also asked Mr Y how the customers react when they wish to deposit cash to their bank account and are asked about the origin of the funds. He stated that in this case, when compared to asking CDD questions, there are more of those customers who become irritated. According to Mr Y, it is kind of a primitive reaction: the customer may feel like he/she is suspected of something or that he/she is not trusted. However, most customers react positively when they are asked about the origin of their funds, and they understand why those questions are asked. (Mr Y, interview 11.11.2015.) An "origin of the funds" –document, which customers are asked to fill out, is commonly used in many banks.

I asked Mr Y how deposits at ATMs are regulated and monitored. He stated that the maximum single deposit is 5,000€, and again, deviations are reacted to regardless of the channel. (Mr Y, interview 11.11.2015.)

4.6 Reporting obligation and suspension of a transaction

Having fulfilled the obligation to obtain information, banks must immediately report a suspicious transaction or a suspicion of terrorist financing to the FIU. Banks are obliged to give the FIU, free of charge, all the necessary information and documents that could be significant in clearing the suspicion. (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Section 23.) If the customer is connected with a state whose system of detecting and preventing money laundering and terrorist financing doesn't meet the international standards, banks must, in order to fulfil the *enhanced reporting obligation*, make a report to the FIU in cases where:

1) the customer does not provide the bank with a clarification that they have requested to fulfil the obligation to obtain information

2) they consider this clarification to be unreliable

3) the clarification obtained by the bank doesn't provide sufficient information on the grounds for the transaction and on the origin of funds

4) the legal person can not be identified

5) the beneficial owner can not be identified or established in a reliable manner

(Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008.)

To be able to recognize unusual and suspicious transactions, it is important that CDD has been adequately conducted. It is all based on "knowing your customer". When the bank detects a suspicious transaction, it has the obligation to clarify the background of that transaction along with the origin of funds involved in that transaction. If the transactions still seems suspicious, even after obtaining more information on it, the bank has to submit a report of suspicious transaction to the FIU. A suspicious transaction report is not an official police report by its nature, and the bank doesn't have to know what crime the funds involved are related to. (Financial Supervisory Auhtority 2010, 38-39.)

Banks must suspend a transaction for further inquiries or refuse to conduct a transaction if the transaction is suspicious, or if they suspect that the funds involved are used for terrorist financing or an attempt to do so. However, if it is not possible to refrain from conducting the transaction, or if refusing to conduct the transaction is likely to hinder finding out the beneficial owner of the transaction, banks may carry out the transaction and then make the report afterwards. A commanding police officer working at the FIU may give the bank an order to refrain from conducting transactions for no more than five working days, if that is necessary for detecting or preventing money laundering or terrorist financing. (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Section 26.)

Banks are liable for the financial loss sustained by their customers only if they have failed to carry out such CDD measures as can be reasonably required from them, considering the prevailing circumstances. (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Section 39). Therefore as long as the banks comply with the CDD rules, they shouldn't be worried about being liable for customers' financial loss sustained as a result of clearing a transaction, reporting a suspicious transaction or suspending or refusing to conduct a transaction.

I asked Mr Y how often Bank X reports suspicious transactions to the FIU, but understandably he could not answer the question. I also asked how often Bank X has to refuse to e.g. open an account. He stated that "It is only on rare occasions that we have to refuse to open an account. The reason for refusal is pretty much always the fact that we are not provided with sufficient information" (Mr Y, interview 11.11.2015). Whenever Bank X has to refuse to open an account, the customer is simply told that he/she is not welcomed as a customer due to missing documents, if that's the case. The customer is never told that the bank is considering making a suspicious transaction report. (Mr Y, interview 11.11.2015.)

4.7 Training and protecting employees

Banks have to provide their empolyees with proper training in order to ensure compliance with the provisions of the AML Act. Banks must have internal instructions in place concerning CDD procedures, fulfilment of the obligation to obtain information, and fulfilment of the reporting obligation. In addition to the training obligation, banks have to take appropriate and adequate measures to protect the employees who submit suspicious transaction reports. (Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008, Section 34.) It is especially important to train those employees who work closely with customers and product development, along with clearing, custody, and payment systems. It is also strongly recommended to keep training records. (Financial Supervisory Authority 2010, 17.)

According to the AML Act, banks may not disclose the making of a suspicious transaction report to the customer subject to the suspicion. (Financial Supervisory Authority 2010, 18). However, it may be intimidating for an employee to make a report of suspicious transaction even if he/she doesn't disclose the reporting to the customer. If the suspicious transaction report leads to police investigations, the customer subject to the suspicion might be able to guess who made the report — especially if the employee refused earlier to conduct the suspicious transaction. Thus the bank should ensure that the customer doesn't get any information concering the identity of the employee who made the report (Financial Supervisory Authority 2010, 18).

The employees in Bank X are trained on a regular basis. "We have had traditional training courses, but nowadays online training courses are commonly used. The employees are also monitored to ensure that they have completed the courses. It is all documented." (Mr Y, interview 11.11.2015.) When it comes to protecting the employees who submit suspicious transaction reports, Bank X "has never needed to use any special measures to protect the employees" (Mr Y, interview 11.11.2015). It is never disclosed to the customer if a suspicious transaction report is made. Neither can the customer link the report – if it leads

to investigations – to the employee who submitted it. If an employee was to be threatened, the police would come along. (Mr Y, interview 11.11.2015.)

4.8 Cost efficiency

I was interested in knowing whether the CDD procedures are perceived only as a time consuming cost, or if they bring any benefits to the bank. I also wondered if the government finances any of the bank's costs arising from the AML and CTF activities. According to Mr Y, CDD might have first been perceived as inconvenient and frustrating, but nowadays the positive sides of it can be found. "The more we know about our customers, the better we can serve them" (Mr Y, interview 11.11.2015). The government doesn't help covering the costs arising from the procedures, though. When asking about the most challenging thing in applying the AML Act in practice, Mr Y stated: "The most challenging thing has been the development of sufficient monitoring systems. Also the fact that the information has to be available in all channels has brought some challenges" (Mr Y, interview 11.11.2015).

4.9 Criticism

AML laundering laws have also been seen as pointless. According to Daniel Mitchell (2012), "They impose very high costs and force banks to spy on their customers, but they are utterly ineffective as a weapon against criminal activity". The main point of Mitchell's article is that AML rules hurt the poor most of all: of those without a bank account, 25% said high cost to be a factor. One of the reasons the costs are so high is that "banks incur regulatory expenses for every customer, in large part because of anti-money laundering requirements, and then pass those on to consumers" (Mitchell 2012).

John Walker, the CEO of Crime Trends Analysis in Australia, was interviewed by David Smith for an article that was published in Economy Watch in 2011. Walker strongly criticized the current measures taken to tackle money laundering. "The concentration on money laundering serves the wealthy countries well, because it is based in the concept of 'suspicious' transactions. It

is dead easy for a white collar criminal to make transactions non-suspicious, so the burden falls on those people who peddle drugs at the retail end of the market" (Smith 2011). Walker suggests that a return to focussing on the original crime – and particularly to the involvement of the legal and accounting professions in those crimes – would be more effective than what is being done now (Smith 2011). Walker has his point. There is barely any data available concerning whether money laundering and terrorist financing have decreased due to the AML and CTF laws. However, as stated earlier, a money laundering investigation is often the only way to locate the hidden assets and establish the identity of the criminals responsible.

Jon Matonis (2013) discusses the fundamentality of money laundering in his article "Money Laundering is a Financial Thoughtcrime". He states that "Money laundering has been called the *thoughtcrime* of finance. Isn't it really just banking with someone's possibly nefarious intentions attached to the act? It is like buying a drive-thru donut in a stolen vehicle. The theft of the vehicle may have been illegal and immoral but the act of purchasing a donut is not" (Matonis 2013). According to him, money laundering is not a pre-crime but rather a post-crime. He also states that "it is difficult to identify the victim, other than the bank shareholders that must expend millions of dollars for the proactive compliance required as the state's deputized enforcers" (Matonis 2013). Matonis's article was published in American Banker –magazine, and thus his opinion is not very surprising.

Michelle Frasher (2015) discusses in her article, which was also published in American Banker, the duality of data in finance. "The dual nature of financial data means that it is simultaneously governed by two regimes: anti-money-laundering and counter-terrorism finance laws that seek to protect the financial system from fraud, crime, and political violence; and data protection and privacy laws that seek to protect an individual's identity and choices from government and private abuse." She states that multinational banks may find it difficult to comply with one without violating the other, especially when different countries

prioritize different regimes. Thus banks must be especially careful when handling CDD data.

5 CONCLUSION

Money laundering is a worldwide issue as it is a consequence of almost all profit generating crime. Criminals try to make their illegally-gained funds appear legal so that they can use them without raising suspicion. Due to the illegal nature of money laundering, it is difficult to estimate the total amount of money that goes through the laundry cycle. There is not accurate data available at all. However, it has been estimated that the amount of money laundered globally per year is 2 – 5% of global GDP, or 800 billion – 2 trillion in US dollars. In Finland, most laundered money originates from economic crimes, whereas globally most originates from drug related crimes.

Traditionally money laundering comprises three stages: placement, layering, and integration. The placement stage represents the initial entry of the illicit cash or proceeds of crime into the financial system. Layering stage involves stratifying the financial transaction. In the integration stage the seemingly legitimate funds are integrated into the perpetrators life. All these stages involve using different methods. In addition to using traditional methods, such as co-mingling illicit funds with sales receipts of a legitimate cash focused business, the using of modern money laundering methods is increasing. Technology is heavily involved in the modern money laundering methods, which makes the tracing of illicit funds more difficult.

Financial service providers, among others, are used by criminals as intermediaries to launder their illicit money. It is crucial for the criminals to get their illegally-gained funds into the legal financial system. However, placing large amounts of money into the legitimate financial system may arise suspicions: in this placement stage, criminals are the most vulnerable to getting caught. International standards, laws and regulations concentrate on the prevention of money laundering, and therefore it is highlighted that financial service providers – as well as others subject to the reporting obligation – should recognize customers' unusual activities and report suspicious transactions. To

be able to recognize unusual activities, banks must know their customers well enough.

The FATF has created a series of recommendations on combating money laundering and financing of terrorism. The recommendations have been adopted by over 190 countries. Also the EU rules in the area of combating money laundering and financing of terrorism are largely based on standards created by the FATF. The Finnish AML Act is then again based on the EU rules. The act applies to, among others, banks. The Financial Supervisory Authority is responsible for ensuring that the procedures, risk management and internal control of banks meet the statutory requirements. Whenever the bank has a suspicion of money laundering or terrorist financing it is obliged to report the suspicion to the Financial Intelligence Unit.

The key principles of the AML Act are Customer Due Diligence (CDD) and a risk-based approach to money laundering and terrorist financing. CDD means the procedures related to customer identification, knowing one's customer, and ongoing monitoring. Banks must have sufficient information on their customers' activities, financial status, banking practices, and purpose for which the services are used. Banks need to find out what kind of services their customers need. Furthermore, the law requires banks to ask where their customers' incoming money comes from and what the money is going to be used for. A risk-based assessment means that banks have internal operational methods and processes in place, adequate with the nature and size of their operations, for assessing the risks of money laundering and terrorist financing related to their customers, services and products.

I interviewed the service manager Mr Y of a Finnish bank (called Bank X in the thesis) to see how the CDD measures are applied in practice. Unfortunately Mr Y was not allowed to give very accurate answers. Due to the vague answers, I had difficulties to answer the research question number 3. However, I also interested to know how customers react to questions about their political influence, the origin of their funds, and so on. When I worked a cashier service officer, I noticed how some customers got irritated when they were asked these

personal questions, and wondered if this was the case in Bank X, too. According to the service manager, Mr Y, most customers react positively and understand why such questions are asked. However, there are still customers who don't quite understand why the origin of their funds is any one the bank's business. Thus it is important that the customers are informed about the AML Act and the fact that banks are obliged by the law to know their customers.

The AML laws have also been criticized as expensive yet ineffective. They are based on the concept of suspicious transactions, and "it is dead easy for a white collar criminal to make transactions non-suspicious" (Smith 2011). Applying CDD measures is also time-consuming. In addition to that, banks have had challenges in developing their monitoring systems to a sufficient level. However, as Mr Y stated, where CDD might have first been perceived as inconvenient and frustrating, now the positive sides of it can be found. The more the bank knows about their customers, the better the customers can be served.

5.1 Self-evaluation

As stated in the introduction, the purpose of this thesis was not to look for a solution to a problem, but rather to come up with an information package on money laundering and what measures banks must take in order to prevent money laundering. The idea was to collect information from various sources in order to identify the main points in the anti-money laundering area. I think I managed to gather the most substantial information to this thesis about money laundering, money laundering prevention and how banks should apply the AML Act. I collected information from various sources that were as recent as possible, and which I considered to be realiable. Unfortunately I had to keep some of the topics rather brief in order to keep the thesis focused. The more research I did on money laundering, the more interested I became in it: it would be interesting to do research on whether money laundering and terrorist financing have decreased due to the AML laws and regulations. It would also be interesting to do research on how banks' monitoring systems could be developed to be more effective. As discussed in the chapter 3.5, Sweden's Financial Supervisory Authority fined two big banking groups for non-

compliance with the AML and CTF legislation. Thus it can be concluded that even big banks lack effective systems to track suspicious transactions.

I wished I could have approach the topic of money laundering prevention from a more interesting point of view as this thesis is now basically a literature / law review including an interview to support the theory. However, the practical part of the thesis was very difficult to conduct. The bank where I worked as a cashier service officer didn't agree to give any information, whereas the service manager whom I interviewed could not give very exact answers to be published. Due to the nature of this subject, it is completely understandable, though. If a more in-depth research was to be done as an assignment given by a bank, for example for developing the monitoring systems, it would have to be made just for the bank, and it could not be published. Overall, I think I was able to collect the most valid points of money laundering prevention to this thesis, and although it wasn't written as assignment for any bank, it could be used as an orientation guide for new employees in the banking sector. Money laundering prevention and CDD is a part of everyday work in a bank, and thus it is important that employees in the banking sector have sufficient information on what they are obliged to do by the AML Act.

SOURCE MATERIAL

About Business Crime Solutions Inc. n.d. Money laundering: A three-stage process. Consulted 18.10.2015 https://www.moneylaundering.ca/public/law/3_stages_ML.php

Basel Institute on Governance. 2015. Basel AML Index 2015 Report. Consulted 5.11.2015 https://index2015.baselgovernance.org/sites/index/documents/Basel_AML_Index_Report_2015.pdf

Chave, C.; Howard Getz, M.; Parker, A. & Seeger, K. 2015. Client Update: Fourth Anti-Money Laundering Directive Comes Into Force. London: Debevoise&Plimton. Consulted 8.10.2005 http://www.debevoise.com/~/media/files/insights/publications/2015/08/08032015a_fourth_anti_money_laundering_directive_comes_into_force.pdf

De Nederlandsche Bank. 2007. Back-to-back loans. Consulted 20.10.2015 http://www.toezicht.dnb.nl/en/2/51-202050.jsp

European Commission. 2006. Week 31: Combating Money Laundering. Consulted 12.10.2015 http://ec.europa.eu/finland/news/press/101/pdf/combating_money_laundring_en.pdf

European Commission. 2015. Confiscation & asset recovery. Consulted 23.10.2015 http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/confiscation-and-asset-recovery/index_en.htm

European Commission. 2015. Financial Crime. Consulted 7.10.2015 http://ec.europa.eu/justice/civil/financial-crime/index_en.htm

European Commission. 2015. Legislative Proposals on financial crime. Consulted 7.10.2015 http://ec.europa.eu/justice/civil/financial-crime/applying-legislation/index_en.htm

European Union. 2015. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L0849

FATF. 2013. The FATF Recommendations: International standards on combating money laundering and the financing of terrorism & proliferation. Consulted 6.10.2015 http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

FATF. 2014. Annual Report 2013 - 2014. Consulted 24.10.2015. http://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF%20Annual%20report%202013-2014.pdf

FATF. 2015. FATF Members and Observers. Consulted 5.10.2015 http://www.fatf-gafi.org/about/membersandobservers/

FATF. 2015. FATF Public Statement – 23 October 2015. Consulted 27.10.2015 http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-october-2015.html

FATF. 2015. Who we are. Consulted 5.10.2015 http://www.fatf-gafi.org/about/

FATF. n.d. Frequently asked questions. Money Laundering. Consulted 26.10.2015 http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223

Federation of Finnish Financial Services. 2013. Miksi pankki kysyy asiakkaan poliittisesta vaikutusvallasta? Consulted 12.11.2015 https://www.fkl.fi/ajankohtaista/tiedotteet/Sivut/Miksi_pankki_kysyy_poliittisesta_vaikutusvallasta.aspx

Federation of Finnish Financial Services. 2014. Kysymyksiä ja vastauksia. Consulted 12.11.2015 https://www.fkl.fi/kannanotot/kysymyksia_ja_vastauksia/Dokumentit/FATCA_QA.pdf

Federation of Finnish Financial Services. 2015. Miksi pankki kysyy? – Oletko poliittisesti vaikutusvaltainen? Consulted 9.11.2015 http://www.fkl.fi/ajankohtaista/tiedotteet/Sivut/Miksi-pankki-kysyy.aspx

Federation of Finnish Financial Services. n.d.. Know Your Customer – why do banks ask? Consulted 5.11.2015 http://www.fkl.fi/en/material/publications/Publications/Know_Your_Customer.pdf

Financial Supervisory Authority. 2010. Standardi 2.4: Asiakkaan tunteminen – rahanpesun ja terrorismin rahoittamisen estäminen. Consulted 5.11.2015 http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Uusi/Documents/2.4.std5.pdf

Financial Supervisory Authority. 2012. Current Provisions. Cosulted 7.10.2015 http://www.finanssivalvonta.fi/en/Supervision/Money_laundering/Current_provisions/Pages/Default.aspx

Financial Supervisory Authority. 2014. Prevention of money laundering and terrorist financing. Consulted 14.10.2015 http://www.finanssivalvonta.fi/en/Supervision/Money_laundering/Pages/Default.aspx

Financial Supervisory Authority. 2015. About us. Consulted 16.10.2015 http://www.finanssivalvonta.fi/en/About_us/Pages/Default.aspx

Financial Supervisory Authority. 2015. Administrative sanctions and other supervisory measures. Consulted 17.10.2015 http://www.finanssivalvonta.fi/en/Supervision/Administrative_sanctions/Pages/Default.aspx

Financial Supervisory Authority. 2015. Customer identification and due diligence. Consulted 5.11.2015 http://www.finanssivalvonta.fi/en/Financial_customer/Financial_services/Pages/customer_identification.aspx

Francis, D. 2014. A Beginner's Guide To Laundering Money. Business Insider UK. Consulted 21.10.2015 http://uk.businessinsider.com/beginners-guide-to-money-laundering-2014-10?r=US&IR=T

HG. org. n.d.. What is Money Laundering and Why is It Illegal. Consulted 21.10.2015 http://www.hg.org/article.asp?id=31085

Hopton, D. 2009. Money Laundering: A Concise Guide For All Business. Second edition. England: Gower Publishing Limited. Consulted 30.9.2015 http://site.ebrary.com.ezproxy.turkuamk.fi/lib/turkuamk/reader.action?docID=10325932

IMF. n.d. Anti-Money Laundering/ Combating the Financing of Terrorism – Topics. Consulted 15.10.2015 https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm

Kervinen, E. 2015. Pankeille isot maksut heikosta rahanpesun valvonnasta Ruotsissa. Helsinki: Helsingin Sanomat. Consulted 17.10.2015 http://www.hs.fi/talous/a1432008161415

Krp. 2012. Rahanpesun torjunnan parhaat käytänteet. Consulted 11.11.2015 https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/26327_Rahanpesun_torjunnan_parhaat_kaytanteet_27.8.2012.pdf?75eb17742473d288

Krp. 2014. Rahanpesun selvittelykeskuksen vuosikertomus 2014. Consulted 15.10.2015 http://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/28746_Rahanpesun_selvittelykeskuksen_vuosikertomus_2014.pdf?5bd61c742473d288

Matonis, J. 2013. Money Laundering is a Financial Thoughtcrime. American Banker. Consulted 23.11.2015 http://www.americanbanker.com/bankthink/money-laundering-is-financial-thoughtcrime-1058902-1.html

MIT Technology Review. 2013. The Secrets of Online Money Laundering. Consulted 24.10.2015 http://www.technologyreview.com/view/520501/the-secrets-of-online-money-laundering/

Mitchell, D. J. 2012. World Bank Study Shows How Anti-Money Laundering Rules Hurt the Poor. Washington: Forbes. Consulted 13.11.2015 http://www.forbes.com/sites/danielmitchell/2012/04/20/world-bank-study-shows-how-anti-money-laundering-rules-hurt-the-poor/

OPF Partners. 2015. Luxembourg. Fight against money laundering and terrorism financing – two new European instruments. Luxembourg: OPF Partners. Consulted 10.10.2015 http://www.opf-partners.com/wp-content/uploads/2015/06/AMLFT-Two-New-European-Instruments_20150609.pdf

Out-Law. 2015. New EU anti-money laundering directive to come into force from 26 June. Consulted 8.10.2015 http://www.out-law.com/en/articles/2015/june/new-eu-anti-money-laundering-rules-to-take-effect-from-26-june/

Poliisi. n.d. Kansainvälinen yhteistyö. Consulted 15.10.2015 https://www.poliisi.fi/keskusrikospoliisi/rahanpesun_torjunta/kansainv%C3%A4linen_yhteistyo

Poliisi. n.d. Rahanpesuilmoituksen tekeminen. Consulted 16.10.2015 http://www.poliisi.fi/keskusrikospoliisi/rahanpesun_torjunta/rahanpesuilmoituksen_tekeminen

Poliisi. n.d. Rahanpesun selvittelykeskus. Consulted 16.10.2015 http://www.poliisi.fi/keskusrikospoliisi/rahanpesun_torjunta/rahanpesun_selvittelykeskus

Poliisi. n.d. Rahanpesun torjunta. Consulted 12.10.2015 http://www.poliisi.fi/rahanpesu

Reuters. 2015. Nordea, Handelsbanken fined over money laundering breaches. Consulted 17.10.2015 http://www.reuters.com/article/2015/05/19/nordea-bank-handelsbanken-fsa-idUSL5N0YA1MS20150519

Sahavirta, R. Rahanpesu rangaistavana tekona. 2008. Jyväskylä: Gummerus Kirjapaino Oy.

Sharman, J. C. 2011. The Money Laundry: Regulating Criminal Finance in the Global Economy. New York: Cornell University Press.

Sisäministeriö. 2015. Rahanpesun ja terrorismin rahoituksen torjunta. Consulted 6.10.2015 http://www.intermin.fi/fi/turvallisuus/rikostorjunta/talousrikollisuus_ja_harmaa_talous/rahanpesun_ja_terrorismin_rahoituksen_torjunta

Smith, D. 2011. Black Money: The Business of Money Laundering. Economy Watch. Consulted 13.11.2015. http://www.economywatch.com/economy-business-and-finance-news/black-money-the-business-of-money-laundering.08-06.html

Solicitors Regulation Authority. 2014. Cleaning up: Law firms and the risk of money laundering. Consulted 20.10.2015 http://www.sra.org.uk/risk/resources/risk-money-laundering.page

Talousrikos. n.d. Rahanpesurikokset. Asianajotoimisto Finsta Oy. Consulted 15.10.2015 http://www.talousrikos.fi/tietoa/rahanpesurikokset/

The Egmont Group. n.d.. About the Egmont Group. Consulted 15.10.2015 http://www.egmontgroup.org/

Turner, J. E. 2011. Money Laundering Prevention: Deterring, Detecting, and Resolving Financial Fraud. New Jersey: John Wiley & Sons, Inc.

UNODC. n.d. Money-Laundering and Globalization. Consulted 25.10.2015 https://www.unodc.org/unodc/en/money-laundering/globalization.html

Uusi Suomi. 2015. Oudot kyselyt pankissa hämmentävät suomalaisia – Tässä selitys. Consulted 12.11.2015 http://www.uusisuomi.fi/kotimaa/109246-oudot-kyselyt-pankissa-hammentavat-suomalaisia-tassa-selitys

Verohallinto. 2015. FATCA-sopimus astui voimaan. Consulted 12.11.2015 https://www.vero.fi/fi-FI/Tietoa_Verohallinnosta/Tiedotteet/Yritys_ja_yhteisoasiakkaat/FATCAsopimus_astui_voimaan(35689)

Laws and Regulations:

Act on Detecting and Preventing Money Laundering and Terrorist Financing 503/2008 http://www.finlex.fi/en/laki/kaannokset/2008/en20080503.pdf

Directive (EU) 2015/849 on preventing the use of the financial system for money laundering or terrorist financing http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN

Regulation (EU) 2015/847 on information on the payer accompanying transfers of funds http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0847&from=EN

The Criminal Code of Finland 39/1889 https://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf

Interview:

Mr Y. 11.11.2015. Bank X. Turku.

Figures and tables:

Figure 1. Caon, V. Banco Madrid hit by BPA money laundering storm. 2015. InvestmentEurope. Consulted 23.11.2015 http://www.investmenteurope.net/regions/spainportugal/banco-madrid-hit-by-bpa-money-laundering-storm/

Figure 2. UNODC. n.d.. The Money-Laundering Cycle. Consulted 23.11.2015 http://www.unodc.org/unodc/en/money-laundering/laundrycycle.html

Figure 3. Basel Institute on Governance. Country map. Consulted 23.11.2015 https://index2015.baselgovernance.org/map

Figure 5. Kuustie. 2015. Interrelation between legislation and the ones the law applies to

Tables 1 - 4. Krp. 2014. Rahanpesun selvittelykeskuksen vuosikertomus 2014. Consulted 15.10.2015 http://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/28746_Rahanpesun_selvittelykeskuksen_vuosikertomus_2014.pdf?5bd61c742473d288

Interview questions

Haastattelun pohjana käytetään lakia rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä (503/2008)

Asiakkaan tunteminen ja riskiperusteinen arviointi

”Ilmoitusvelvollisella tulee olla rahanpesun ja terrorismin rahoittamisen riskienhallintaa koskevat, ilmoitusvelvollisen toiminnan luonteeseen ja laajuuteen nähden riittävät menetelmät. Ilmoitusvelvollisen on rahanpesun ja terrorismin rahoituksen riskejä arvioidessaan otettava huomioon toimialaansa, tuotteisiinsa, palveluihinsa, teknologian kehitykseen, asiakkaisiinsa ja näiden liiketoimintaan ja -toimiin liittyvät rahanpesun ja terrorismin rahoituksen riskit.”

- Minkälaista riskiarviointia Pankki X käyttää?
- Minkälaisiin riskiluokkiin asiakkaat luokitellaan?
- Miten toiminta on organisoitu? Kuka vastaa riskien hallinnan ja sisäisen valvonnan järjestämisestä?
- Miten varmistetaan, että sovittuja periaatteita noudatetaan yhtenäisesti koko pankkiryhmässä?

Selonottovelvollisuus ja jatkuva seuranta

”*Ilmoitusvelvollisen on hankittava tietoja asiakkaansa toiminnasta, tämän liiketoiminnan laadusta ja laajuudesta sekä perusteet palvelun tai tuotteen käyttämiselle.*

Ilmoitusvelvollisen on järjestettävä asiakkaan toiminnan laatuun ja laajuuteen sekä riskeihin nähden riittävä seuranta sen varmistamiseksi, että asiakkaan toiminta vastaa sitä kokemusta ja tietoa, joka ilmoitusvelvollisella on asiakkaasta ja tämän toiminnasta.

Ilmoitusvelvollisen on erityisesti kiinnitettävä huomiota liiketoimiin, jotka rakenteeltaan tai suuruudeltaan taikka ilmoitusvelvollisen koon tai toimipaikan osalta poikkeavat tavanomaisesta. Samoin on meneteltävä, jos liiketoimilla ei ole ilmeistä taloudellista tarkoitusta tai ne eivät sovi yhteen sen kokemuksen tai tietojen kanssa, jotka ilmoitusvelvollisella on asiakkaasta. Tarvittaessa liiketoimeen liittyvien varojen alkuperä on selvitettävä.”

- Minkälaisia kysymyksiä Pankki X kysyy uutta asiakassuhdetta perustettaessa? Kuinka usein perustietoja päivitetään?
- Miten asiakkaat suhtautuvat, kun heiltä tiedustellaan yksityiskohtaisia tietoja heidän rahaliikenteestään, poliittisesta vaikutusvallastaan, jne.?
- Kerrotaanko asiakkaalle, miksi pankki kysyy?

- Miten jatkuva seuranta on järjestetty?
- Miten tunnistetetaan tavanomaisesta poikkeavat liiketoimet?
- Miten asiakkaat suhtautuvat, kun heiltä tiedustellaan varojen alkuperää suurta käteistalletusta tehtäessä?

Tehostettu asiakkaan tuntemisvelvollisuus

”*Ilmoitusvelvollisen tulee noudattaa asiakkaan tuntemista koskevia toimia tehostetusti, jos asiakkaaseen, palveluun, tuotteeseen tai liiketoimeen liittyy tavanomaista suurempi rahanpesun tai terrorismin rahoittamisen riski taikka jos asiakkaalla tai liiketoimella on liittymäkohta valtioon, jonka rahanpesun ja terrorismin rahoittamisen estämis- ja selvittelyjärjestelmä ei täytä kansainvälisiä velvoitteita.*”

- Kenen laatimaa / mitä listaa korkean riskin maista käytetään? (FATF, Basel AML Index, Suomen valtioneuvoston päätös, EU:n ja YK:n finanssipakotelistat jne.)

Velvollisuus tehdä ilmoitus epäilyttävästä liiketoiminnasta, liiketoimen keskeyttäminen tai siitä kieltäytyminen

- Joudutaanko ilmoituksia epäilyttävästä liiketoiminnasta tekemään usein?
- Kuinka usein esimerkiksi tilin avaamisesta joudutaan kieltäytymään? Mikä on tällaisessa tapauksessa tyypillinen perustelu kieltäytymiselle?
- Miten asiakkaat suhtautuvat, jos liiketoimesta kieltäydytään? Miten asiakkaalle perustellaan luontevasti liiketoimesta kieltäytyminen, kun hänelle ei saa paljastaa, että liiketoimesta on tehty ilmoitus?

Työntekijöiden koulutus ja suojeleminen

”Ilmoitusvelvollisen on huolehdittava, että sen työntekijät saavat asianmukaisen koulutuksen tämän lain ja sen nojalla annettujen säännösten noudattamisen varmistamiseksi. Ilmoitusvelvollisen tulee toteuttaa asianmukaiset ja riittävät toimenpiteet niiden työntekijöiden suojelemiseksi, jotka tekevät 23 tai 24 §:ssä tarkoitetun ilmoituksen.”

- Miten henkilökuntaa käytännössä koulutetaan rahanpesun estämisen saralla?
- Miten niitä työntekijöitä suojellaan, jotka ovat tehneet ilmoituksen epäilyttävästä liiketoiminnasta?

Yleisiä kysymyksiä

- Miten talletusautomaattien käyttöä valvotaan / rajoitetaan?
- Rahoittaako valtio pankin valvontatoimia rahanpesun estämiseksi, vai ovatko kulut vain pankin vastuulla?
- Onko asiakkaan perinpohjaisesta tuntemisesta hyötyä myös pankille esimerkiksi myynnin kohdentamista ajatellen, vai koetaanko tietojen kysely lähinnä aikaavievänä kulueränä?
- Minkälaisia haasteita rahanpesun estämiseen pankissa liittyy?

Lisäksi

- Onko mahdollista saada ”selvitys varojen alkuperästä” -lomaketta opinnäytetyön liitteeksi?
- Onko mahdollista saada liitteeksi myös jonkinlaista asiakkaan perustietolomaketta?

Know Your Customer - why do banks ask?

Banks must know their customers

According to Finnish law, banks are required to comply with the customer due diligence standards, which means that banks must identify and know their customers. Besides personal details of the customer, the bank must have sufficient information on the customer's activities, financial position, banking practices, and purpose for which the services are used. In practice, banks must verify their customers' identity from an official identity document and find out what kind of services the customer needs. Moreover, the law requires banks to ask where incoming money comes from and what the money is going to be used for.

To find out the source of incoming money the bank may ask the customer for not only a written statement but also documents evidencing business operations, registration or any other proof (eg deed of sale or letter of reference from another bank) that may help the bank to verify the source if funds and the purpose for which the funds are used.

Any information or documentation given to the bank is treated in confidence in compliance with the Finnish guidelines on banking secrecy

Acceptable proof of identity

Before establishing a banking relationship, the bank must verify the potential customer's identity from a reliable source.

Personal customers

The following documents are considered reliable proof of identity for banking purposes in Finland, providing the documents are in force and issued by Finnish authorities:

1) Passport
2) Identity card (also temporary)
3) Driving licence
4) Photo-bearing identity card issue issued by the Social Insurance Institution of Finland
5) Alien's passport
6) Diplomatic passport
7) Refugee's travel document

Valid passport is the only foreign-issued document accepted as reliable proof of identity.

National identify documents used in the EU and EEA as travel documents may also be accepted as proof of identity at banks, if their authenticity can be verified, but even citizens of the EU and EEA countries may be asked for further documents to support identification.

For instance, if it is not possible to verify either the safety features or the validity of a travel document acceptable in the Schengen area, the bank may ask the customer to present a passport.

The bank must be able to reliably identify the customer from the identity document provided. Driving licences issued outside Finland are not accepted as evidence of identity at Finnish banks.

Corporate customers

The bank must identify its corporate customers by means of documents issued by a reliable and impartial source, eg an extract from the trade register. Moreover, the bank must be given information on the company's business, turnover, corporate structure and shareholders. To supplement this information, the bank is entitled to ask for financial statements, articles of association and any other documents considered necessary by it.

If the corporate customer is not Finnish, the bank may ask the customer to provide an extract from the company register of the country concerned, the company's articles of association, financial statements or a letter of reference issued by a correspondent bank of the Finnish bank. The documents required may vary case by case depending on the corporate structure and the country of registration.
When it provides means of strong authentication for use in electronic communication, the bank complies with the provisions of the relevant special statute regarding documents eligible for verification of the customer's identity.

Politically exposed persons

Finnish legislation also requires banks to know whether the customer is a *politically exposed person* or a *family member* of such person or a *close business partner* of such person.

Politically exposed person is a person that works or has in the past twelve months worked for another state as

- head of state, minister, member of parliament, member of the highest court, member of the highest policymaking body auditing state finances, member of central bank board, ambassador or chargé d'affaires, general officer, executive of a fully state-owned company

Family members of a politically exposed person comprise:

- spouse, children and their spouses, parents

Yet Finnish politicians working in Finland are not considered politically exposed persons for this purpose

Information on funds involved in transactions

The bank is required to have sufficient information on the customer's banking practices and the purpose for which the banking services are used. This information is recorded in an outline drawn up by the bank together with the customer both before the services are agreed on and during the customer relationship. In this setting, the bank may ask the customer for information on income or any other circumstance that may help the bank to outline the customer's need for services. If in any event a transaction to be completed deviates from the customer's day-to-day banking or way of using the services, the bank is required to inquire about the purpose of the transaction and the source of the funds involved in the transaction. The bank may also need to see agreements or other documentation relating to such transaction.

Payer information

Disclosure of payer information has been governed also in Finland by an EU Regulation since 2008. The decree requires banks to make sure that all incoming and outgoing payments are accompanied by the payer information set out in the decree. This means that the bank is also required to check the identity of persons making cash payments at the bank. As a result, persons making cash payments at the bank need to be prepared to prove their identity when making the payment. If the payer information is incomplete, the bank is not allowed to credit the payment to the beneficiary,

Rejecting a transaction

The bank is required to ask for such information as is needed by it to become convinced of the customer's identity and nature of transactions. The extent of the information needed, including documents or other evidence of the source of funds, is determined by the bank according to Finnish law. If it does not get the information needed to support the establishment of a customer relationship or execution of a transaction, the bank must reject the transaction.

Additional information

Additional information on customer identification in banks and official documents related to the identification requirement is available through the following sources:

www.pankkiturvallisuus.fi
www.fkl.fi
www.rahanpesu.fi

FK|Finanssialan Keskusliitto
FC|Finansbranschens Centralförbund
Federation of Finnish Financial Services